

# On User Choice for Android Unlock Patterns

Marte Loge  
NTNU, Norway  
marte.loge@gmail.com

Markus Duermuth  
Ruhr-University Bochum, Germany  
markus.duermuth@rub.de

Lillian Rostad  
NTNU, Norway  
lilliaro@ntnu.no

**Abstract**—Android Unlock Patterns are one of the most widely used graphical password schemes. However, the scheme’s security is limited by users not choosing patterns uniformly but with a specific bias. In this work we take a closer look at this bias, in particular how personal traits influence the chosen patterns. We conducted a user study with 800 participants and demonstrate that certain factors such as age, gender, and experience in IT significantly influence the strength or length of the chosen patterns. This has implications both for how we can help users to select stronger patterns and for forensic applications.

## I. INTRODUCTION

Over the last decade, mobile phones have evolved from simple tools for making voice calls to powerful computers which can be used to access emails and social media, make payments, access online banking, and store private as well as work-related sensitive information. User authentication helps protecting the sensitive information stored on the device. Authentication schemes commonly used on smartphones include (i) knowledge-based schemes, mostly PINs and (graphical) passwords; (ii) biometric schemes, mostly fingerprint recognition (recent iPhone models and other high-end models) and face recognition (e.g. offered on Android since version 4.0); (iii) security tokens are rarely used on smartphones (however, a smartphone is commonly used as second factor to authenticate to another device or account). PINs and Android Unlock patterns are the most frequently used schemes, but studies are not conclusive to which one is used more often (cf. [27], [17], [16]).

User-chosen authentication secrets are known to be relatively predictable, regardless if they are PINs [10], passwords [20], or graphical passwords [12], [14], [26], and can therefor be determined by guessing attacks. Even more, certain observable properties of a person have been shown to influence the selected authentication secret. This effect has been demonstrated for PINs [10], where it was demonstrated that knowledge of a person’s birthday significantly accelerates guessing the person’s PIN, for passwords [11], where it was shown that knowing background information such as birthday, occupation, and friends can improve guessing success by around 5%, and for the graphical password scheme PassFace [12], where it was

found that faces were selected with a strong bias based on race and gender.

In this work, we study the effect that personal traits of a user have on his selection of Android Unlock Patterns. This was, to the best of our knowledge, never studied before, the only exception being independent and concurrent work by Aviv et al. [7] which studied the influence of collection methods and personal traits on the collected patterns. However, they only studied the influence of personal traits on specific characteristics of the patterns, such as length, starting point, and occurrence of crosses and knight-moves. In this work, we use a Markov model-based meter to approximate the strength of individual patterns and thus being able to analyze the influence of personal traits on the strength of individual patterns.

We conducted an online survey that asked users to use the Android Unlock Pattern scheme to secure access to (i) a shopping account, (ii) a smartphone, and (iii) a bank account. In addition, we asked participants to answer a questionnaire which contained standard demographic questions, and specifically questions about factors that we believed may influence the strength of the chosen patterns, such as gender, background in IT or IT security, handedness, and others. We show that age and gender have a significant influence on the average strength of the patterns chosen (both male users and younger users choose stronger patterns on average), while somewhat surprisingly having experience in IT or IT security did not have a statistically significant influence (but still had a statistically significant influence on the pattern length).

Our work helps us to understand some of the factors behind weak user-selected authentication secrets, and may hint at directions to help users avoiding weak patterns. Our work also shows directions to speed up the guessing of authentication secrets in forensics, but more work is required before usable results can be obtained.

*Outline.* We discuss related work in Section II, before describing details about the Android Unlock Pattern scheme in Section III. We present the design of our user study in Section IV and the results in Section V. We discuss these results in Section VI and conclude with some final remarks in Section VII.

## II. RELATED WORK

*Graphical passwords.* Graphical passwords have the potential to offer easier-to-use authentication, as there is indication that graphical information is easier to remember by humans [13]. Recently they found wide-spread adoption specifically on

mobile devices, as they are particularly well-suited for touch-screen use, while text-based passwords are much less suited for devices without a physical keyboard.

The first description of a graphical password scheme goes back to a patent by Blonder [8], which describes a scheme where a user needs to select specific points in an image. This scheme is an example for a *cued-recall based scheme*, other examples include BDAS [15] and PassPoints [29], [30], [31]. Presumably the most widely used cued-recall based scheme is Windows Picture Password, which is quite similar to Blonder’s original proposal and to the PassPoints scheme.

The classical example for a *recall-based graphical password scheme* (without a cue) is the draw-a-secret scheme (DAS) [19], where one draws free-handed on a grid. In 2007, Tao and Adams [23] modified this original idea by snapping the drawn lines to the intersections of a grid, thus removing many of the problems of ambiguities of the DAS scheme and making it much easier to use, calling the resulting scheme Pass-Go. This scheme was adopted, with some restrictions, for use in the Android mobile phones in 2008, which we will describe in more detail in Section III.

Finally, *recognition-based schemes* are based on recognizing a previously seen object, instead of recalling information. One of the classical examples is the PassFace scheme, where the user selects several pictures of faces, and has to select these faces among a number of decoy images for authentication. Several related schemes have been deplored, but to the best of our knowledge there is no scheme with significant adoption.

*Security of graphical passwords.* For the DAS scheme, Oorschot and Thorpe [24] analyzed the security based on mirror symmetric fragments. They constructed dictionaries that improve guessing attacks against graphical passwords and estimated the realistic space of passwords being exponentially smaller than the theoretical space. Jermyn et al. [19] analyzed the security of the DAS scheme for computer-generated passwords. However, computer-generated passwords are in practice only used for very few accounts, problems being user acceptance and low usability.

For the PassPoints scheme, Dirik et al. [14] investigated the distribution of user’s choices and found substantial bias based on data collected from human users. Thorpe and Oorschot [25] used a more involved method and used click-points collected in a user-study to seed automated methods for predicting likely click-points, further facilitating and improving this kind of attack. Zhao et al. [32] evaluate the security of the graphical password scheme used in Windows 8 and propose effective guessing algorithms against them.

*Android Unlock Patterns.* Uellenbeck et al. [26] evaluated the security of Android Unlock patterns and found substantial bias both in the starting point as well as the path chosen by users. They precisely quantified the security of the scheme and found its security to be lower than that of a uniformly chosen 3-digit PIN. They additionally evaluated the influence of a changed layout and found that layout changes indeed have a substantial influence on the security, even with the same number of nodes. The security of variants was also studied by Aviv et al. [4], who compared Android Unlock Patterns both on the standard  $3 \times 3$  grid and on a  $4 \times 4$ , and found a very

limited increase of security on the larger grid. Arianezhad et al. [3] evaluated a gaze-based variant of the scheme using an eye-tracker, and reported statistics about start- and end-points, frequent stroke directions, and similar for several arrangement of contact points.

The influence of strength meters on user-choice for Android Unlock Patterns was tested by Andriotis et al. [1] and by Song et al. [21], who used a very elaborate study setup.

Attacks beyond guessing attacks were considered by Aviv et al. [5], who used “smudges” left on the smartphone screen while entering a pattern to reconstruct the user’s secret. Andriotis et al. [2] extended this attack by incorporating statistics about patterns typically chosen by users. The accelerometer built into basically all modern smartphones was shown [6] to leak (partial) information about PINs and patterns entered on a smartphone. Von Zezschwitz et al. [28] measured and compared the usability of (assigned) PINs and Android Patterns under a realistic setting over three weeks.

*Individual aspects and security.* A particularly interesting aspect is to what extent the authentication secret is influenced by the person choosing it. Specifically, if observable characteristics of a person influences the secret this can potentially be used to speed up guessing attacks. For text-based passwords, Bonneau [9] found different entropy values for different groups of users. However, due to his data collection method he was unable to look at specific password choices and only observed the resulting distribution of choices, so he could not investigate any further details such as the cause for the differences in strength. Castelluccia et al. [11] found that incorporating a few publicly available datapoints about a user can increase the chance of guessing a password correctly by approx. 5%. In the context of graphical passwords, specifically for the PassFace scheme, Davis et al. [12] showed that the bias in choosing faces significantly depends on gender, race, and subjective beauty of the face.

The work closest to our work is recent and independent work by Aviv et al. [7]. They studied the influence of both collection methods and personal traits on the collected patterns. However, they only reported the influence of personal traits on specific characteristics of the patterns, such as length, starting point, and occurrence of crosses and knight-moves, and did not report on the influence of these traits on the actual strength of individual passwords.

### III. ANDROID UNLOCK PATTERNS

Next we give a brief introduction to the Android Unlock Pattern scheme and describe the pattern strength meter that we used.

#### A. Description

Android Unlock Patterns (AUP) are a restricted variant of the Pass-Go scheme [23], which in turn goes back to Draw-A-Secret (DAS) [19], one of the early graphical password schemes. They were introduced in 2008, are available on all current Android phones, and are widely used. The most common design, which will be used throughout this paper, uses 9 points arranged in a  $3 \times 3$  grid. The user selects a path through these points according to the following rules:

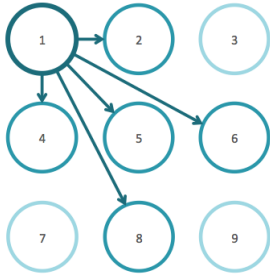


Fig. 1. Points reachable from the top-left node.



Fig. 2. Strength meter examples with score 0.0361 (left) and  $0.114 \cdot 10^{-4}$  (right).

- (i) At least four points must be selected,
- (ii) No point can be selected more than once,
- (iii) Only straight lines are allowed, and
- (iv) All points along a path will be connected (unless it was selected before).

The first rule ensure a certain minimal strength of the resulting patterns, albeit little is known about the exact implications on pattern strength. The other rules presumably resolve ambiguities from graphical representations of the patterns, potentially increasing usability. Figure 1 demonstrates the points reachable from the top-left starting position.

### B. Measuring pattern strength

One can easily enumerate all possible patterns that adhere to the above rules and determine there are 389 112 valid patterns. However, users do not choose their patterns uniformly from this set, and previous work [26] has established that the resulting strength fall substantially short of the theoretical maximum. Different approaches have been used to determine the strength of patterns. We adapt the approach by Uellenbeck et al. [26], which is based on Markov models. We will describe this approach in the sequel.

*Markov Models.* Markov models are based on the observation that subsequent tokens, such as letters in normal text or nodes in the Pass-Go scheme, are rarely independently chosen by humans, but can often be quite accurately modeled based on a short history of tokens. For example, in English texts, the letter following a  $t$  is more likely to be an  $h$  than a  $c$ , and for the Pass-Go scheme, nodes which are close to the current node are more frequently chosen than distant ones. In an  $n$ -gram Markov model one models the probability of the next token in a string based on a prefix of length  $n - 1$ . Hence, for a given sequence of tokens  $c_1, \dots, c_m$ , an  $n$ -gram Markov

model estimates its probability as

$$P(c_1, \dots, c_m) = P(c_1, \dots, c_{n-1}) \cdot \prod_{i=n}^m P(c_i | c_{i-n+1}, \dots, c_{i-1}). \quad (1)$$

The required *initial probabilities*  $P(c_1, \dots, c_{n-1})$  and *transition probabilities*  $P(c_n | c_1, \dots, c_{n-1})$  can be determined empirically from the relative frequencies from training data. One commonly applies further post-processing to the raw frequencies: So-called *smoothing* tries to even out statistical effects, in particular it avoids relative frequencies of 0, as these would yield an overall probability of 0 regardless of the remaining probabilities.

*Strength-estimation using Markov models.* We use Markov models to estimate the probabilities of patterns, and use those probabilities as approximations for their strength. We closely follow the techniques used by Uellenbeck et al. [26]. Their best results were obtained using 3-grams, Laplace smoothing, and using the maximum amount of data available. We train the model on the data collected by Uellenbeck et al. This data was collected in an “adversarial setting”, where users chose patterns to protect an account, and were instructed that the account is under attack by other participants. This setup yields one “defensive” pattern, which is used to protect one’s account, as well as five “offensive” patterns, used to attack other accounts, per user. We used both the “defensive” and “offensive” dataset, overall more than 600 patterns. In particularly, the model is trained on data which was independently collected from the data that we are considering in this work.

These estimated probabilities  $\hat{p}$  can be used directly as a strength measurement. However, a more readable measure is  $-\log(\hat{p})$ , where logarithms are to basis 2. We use this strength measure throughout this work.

Other strength estimators have been used in previous work. All three are based on readily observable characteristics of the patterns. The meter by Sun et al. [22] uses length, length of the drawn pattern, and the number of intersections. The meter by Andriotis et al. [1] uses the length, number of knight moves, number of overlaps, starting point, and number of changes in direction. The meter by Song et al. [21] uses length, number of intersections, and “non-repeated segments”. However, in all three cases there is no theoretical foundation or evaluation for the accuracy of the computation. Thus we refrain from using these metrics.

## IV. USER STUDY

Next we describe the design and pre-testing of our online study.

### A. Study design

We used an online study to collect patterns for the subsequent analysis. Participants were recruited via mailing lists, social networks, and word of mouth. This has the advantage of reaching a relatively large number of participants in a short time, but has the disadvantages that we had little control over participants while filling in the survey (which was mitigated

by rigorous testing of the survey) and little control over the selection of participants (see Section IV-C for statistics about the participants). Data was collected between February and March of 2015 over a time span of 4 weeks.

Different input methods (touchscreen, mouse, pen-on-paper, ...) used by the participant may have an effect on the patterns chosen. For example, using a mouse cursor may allow for a finer control and might facilitate input of more complicated patterns, e.g., those that contain a “knight move”. So we wanted to ensure that the users use a smartphone when participating in the study. We used a third-party package<sup>1</sup> to block participants that were not on a mobile device. The package uses a number of heuristics to decide on the device type, including scanning the user agent string transmitted by the participant’s browser for specific keywords (such as “mobile”, “android”, “windows ce”, “LG”, “wap1.”, ...), and detecting mobile versions of browsers.

We also wanted to make the study easy to access, specifically without requiring the user to install any additional software. We opted for an HTML/JavaScript web application together with the django/python framework. This means the survey can be accessed using any modern web-browser installed on smartphones, and the look-and-feel can be modeled very similar to that of Android Unlock Patterns, without being restricted to Android Phones.

The survey was structured in four stages: (i) General information, (ii) Short introduction to Android Unlock Patterns, (iii) Pattern collection, and (iv) Questions on demographics and device. We provide more information about these stages in the following sections.

*Information.* When entering the survey, all participants were presented with a brief introduction to the study, its goals and purposes, the data usage policy, and the researchers behind the project. More detailed information is linked from this screen. No data is collected before a visitor decides to participate by pressing “Start Survey” as illustrated in Figure 3(a). Clicking the green button starts the study.

*Introduction to Android Unlock Patterns.* Before starting the pattern collection, we need to ensure that participants are familiar with the scheme. Therefore, on the next screen (Figure 3(b)) we provide a brief explanation, and give the participant the possibility to start a more comprehensive training (by pressing “Start training”) or continue with the survey (by pressing “Skip training”). In training mode (see Figure 5(c) in the appendix), the participant can test creating patterns as often as she likes, and optical feedback is provided on the validity of the chosen patterns. After selecting “Continue survey”, the participant leaves the training mode and continues with the pattern collection as described in the sequel.

*Pattern collection.* In the main stage of the study, we ask the participants to create three different patterns for three different scenarios. One pattern for protecting an shopping account, one for unlocking a smartphone, and a third one for protecting a banking account. Those were presented in randomized order. There are two reasons why we ask each participant to create

three different patterns: First, this puts pattern creation in a context. The scenarios were selected to cover different situations with different (perceived) security requirements. Thus we avoid problems that one user creates a relatively weak pattern assuming a context with low security requirements (e.g. as she is using the scheme for her smartphone and doesn’t value the data on her smartphone very high), whereas another participant assumes a context with high security requirements. Second, we hope this prevents, to some extent, data being submitted by participants that just are curious about the survey and rush to finish the survey, introducing noise into the collected dataset.

The pattern selection step follows the original implementation on Android phones as closely as possible. (Note that, while being functional equivalent, the visual appearance of different Android versions can differ quite a lot.) In a first step, a user selects a pattern that meets the requirements (Figure 3(c)). If a selected pattern fails to meet these requirements, we give visual feedback, as well as a textual description of the condition the pattern failed to meet (see Figure 6(e) in the appendix). Once the user selected a valid pattern, in a second step she is required to confirm this pattern by re-typing it. If the confirmation fails, the system gives visual feedback and allows the participant to try again. If she ultimately fails to re-type the correct pattern, it is possible to go back and create a new pattern. The type-and-re-type approach is the same process used when creating a pattern on a Android device. There are several positive aspects by requiring the respondent to re-type the selected pattern before being able to proceed in the survey. First, it stops users that want to rush through the survey without making an effort to submit an honest answer. Second, it also puts the respondent in a situation where it is needed to create a pattern that is possible for the respondent to actually remember, which is an obvious requirement for real-world patterns.

*Demographic questions.* Finally, we ask several questions about the participant’s demographics as well as the used device. One example screen is shown in Figure 3(d), see Figure 7 in the appendix for a more complete list. In the survey, we ask

- for a subjective assessment of the *hand size of the respondent* based on their gender, ranging from small to extra large, illustrated by icons labeled S, M, L, XL;
- for handedness of the participant using labeled icons for left and right;
- for a subjective assessment of the *screen-size* of the device used, with options S, M, L;
- *which hand is used holding the device* during creation of patterns;
- which *finger was used* when creating the patterns, options were thumb, index finger, other;
- for the usual *reading/writing direction* of the participant, illustrated by an arrow, written text, and an example, options were left-to-right, right-to-felt, and top-to-down;
- for the participant’s *gender*, using icons for male and female;
- for the participant’s *age*, using a numerical input field;
- if the participant has *experience in IT or IT security*, as a yes-no question;
- for the current type of *screenlock in use*, if any;
- if the participant has any experience with pattern locks as a yes-no question;

<sup>1</sup><https://code.google.com/archive/p/minidetector/>



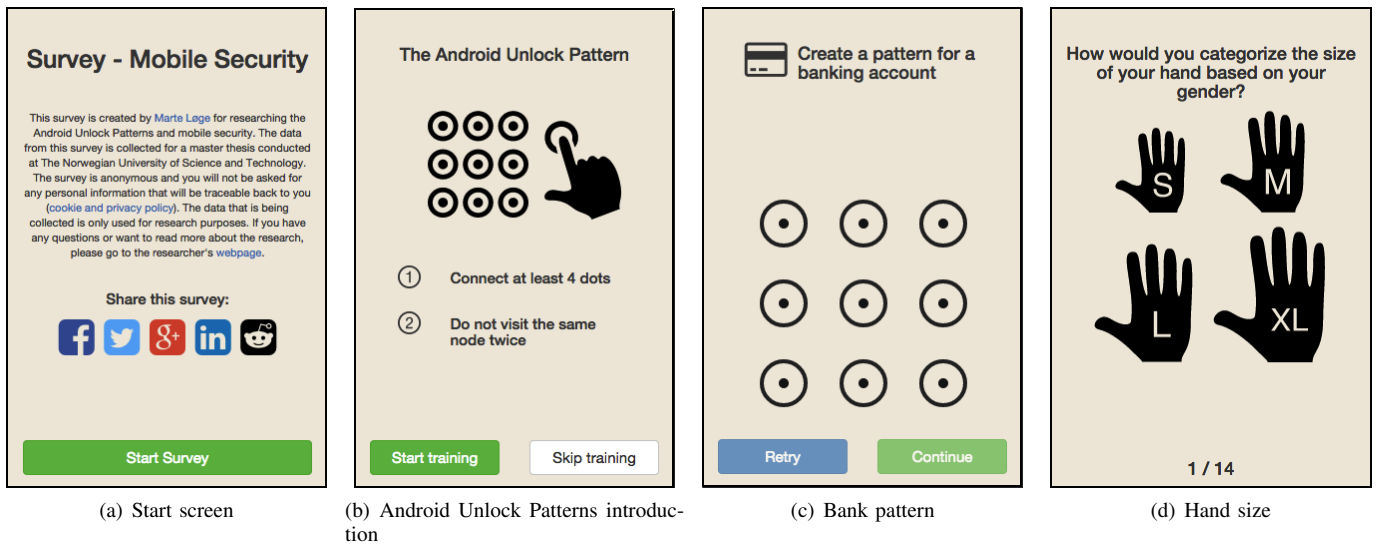


Fig. 3. Selected screens of the survey. More screens are provided in the appendix.

- for the *mobile OS* on the used smartphone (to simplify this task we tried to automatically detect the OS and asked the question “Is this the mobile operating system on your mobile?”), options were yes, no, I don’t know;
- for the *country of origin* of the participant.

We used icons instead of textual lists of alternatives. Our main target device are smartphones, and we believe that icons are easier to interact with on those devices. Icons specifically make it easier for non-natives to quickly complete the survey, and several respondents of a pre-test told us it’s more fun to complete the survey with icons. The icons were tested in a pre-test, see Section IV-B. One final screen thanks the participants for their time.

### B. Pre-test: Testing the survey

We tested the survey in a controlled environment before releasing it to the public, where we would have little control over the participants. Specifically important for us was testing if the chosen icons where understandable to a broad audience. So even before the pre-test we ran a separate test for the icons only. Test subjects were 12 students, 5 female and 7 male. We showed them the icons used, without the question provided (whereas in the study the questions were stated in English). The only questions that caused some irritation were about the screen lock usage, where some symbols were not readily understandable (we replaced it with a textual list to choose options from), and the question about reading/writing direction, where we added explanation in textual form.

The actual pre-test was conducted with 10 students (5 female, 5 male, a majority with an background in IT or IT Security), in-lab but using their own device. The participants were told (i) to speak aloud during the test about their thoughts and reasons for their choices, (ii) that the test was not about their ability to finish the test, (iii) that they could quit the test at any time if they felt uncomfortable.

Based on the feedback provided by the participants while they interacted with the test we made the following changes

to the design (Figures 3, 5, 6, 7 show the final version of the study):

- We simplified the drop-down menu for the country selection, as the original one had graphical flags for each country, which made the component slow and thus hard to use on some devices
- The text for the IT Security question was re-formulated and clarified.
- For the reading/writing direction question we added a textual description and examples to clarify the icons.
- For the screen lock question we replaced the icons with text.
- For the hand-size question, we added that the assessment should be compared to people of the same gender.
- Originally participants did not have to re-type their patterns, and we added that.

### C. Participants

A total of 802 respondents completed the whole survey, and 296 more respondents started the survey but did not complete it (81 left before entering any data, 204 started selecting patterns but quit before reaching the questionnaire, and 11 respondents completed creating patterns but did not complete answering questions). Table I provides a summary of the respondents. As some of the respondents did not answer all demographic questions, some questions have more than 802 answers. A majority of the participants was male (66%), between 20 and 29 years old (62%), has some background in IT or IT security (59%), and is from Norway (64%) or the United States (14%). This is a consequence of the recruitment process via social networks and mailing lists, which addressed a proportionally higher number of students and IT security experts. About 88% of the participants is right-handed, which roughly agrees with estimates in the literature [18]. The vast majority reads and writes from left-to-right (98%), which is a consequence of the predominantly western population; we did not use this feature in the following analysis.

		Total	In %
Gender	male	529	66%
	female	278	34%
Handedness	right	690	88%
	left	97	12%
IT or IT security	expert	470	59%
	non-expert	332	41%
Writing-orientation	left-to-right	792	98%
	right-to-left	8	1%
	top-to-bottom	7	1%
Age	16-19	22	3%
	20-24	331	41%
	25-29	169	21%
	30-34	96	12%
	35-39	82	10%
	40-49	73	9%
Hand-size	50+	30	4%
	small	103	13%
	medium	406	50%
	large	255	31%
Country	extra-large	49	6%
	Norway	517	64%
	USA	115	14%
	Germany	33	4%
	Czech Republic	31	4%
	UK	22	3%
Russia	13	2%	
	Rest (<10 each)	75	9%
Total (*)		802	100%

TABLE I. STATISTICS OF THE PARTICIPANTS. (\*) NOTE THAT 802 PARTICIPANTS COMPLETED THE ENTIRE STUDY, BUT A FEW PARTICIPANTS ANSWERED SOME QUESTIONS BEFORE LEAVING. THUS SOME QUESTIONS HAVE MORE THAN 802 ANSWERS.)

		Total	In %
Screenlock in use	Android Pattern	202	31%
	4-digit PIN	237	36%
	Fingerprint	116	18%
	Password	44	7%
	slide-to-unlock	28	4%
	Other	28	4%
Screensize	Small	108	13%
	Medium	532	65%
	Large	173	21%
Mobile OS	Android	464	58%
	iOS	321	40%
	Windows	16	2%
	Blackberry	1	0%
Used AUP	Yes	526	65%
	No	278	35%
Total		802	100%

TABLE II. STATISTICS OF THE DEVICES USED BY THE RESPONDENTS

#### D. Ethical considerations

The ethics committee of NTNU approved the study and the respective contact person was informed. While there is no ethics committee covering this type of user studies at Ruhr-University Bochum (RUB), federal law and privacy regulations must be obeyed. This study complies with these strict regulations. The data we collect about a participant cannot be linked back to a respondent, as the data is in quite broad categories only. We did not collect any identifiers (IP, device ID, name, or similar), and did not use third-party components that still may log such data. Before any data is recorded the respondents are informed about the purpose of the survey and how the contributed data will be managed, and that they can leave the survey at any time.

### V. ANALYSIS AND RESULTS

Next we describe the results of analyzing the collected patterns.

Scenario	All	AUP experience	No AUP experience
Shopping	7.06	6.81	7.15
Smartphone	6.45	5.95	7.39
Bank	8.08	8.19	7.69

TABLE III. MEDIAN OF PATTERN CREATION TIMES (IN SEC).

#### A. Methodology

Most statistical significance test are performed on strength scores. As there is no reason to believe these follow a normal distribution (in fact a Shapiro-Wilk-Test rejects the null hypothesis of normality with  $p < 10^{-15}$ ), we use the Mann-Whitney U-Test for significance testing and Spearman's rank correlation for correlations on strength scores. Similarly, the Shapiro-Wilk-Test rejects the null hypothesis of normality for both the time to choose a pattern and the length of patterns, thus we use the Mann-Whitney U-Test in these cases as well. As we run several tests against the same dataset we use Bonferonni correction. We claim statistical significance for  $p < 0.05$ , and we indicate possible significant interest for  $p < 0.10$ . We indicate these in the tables with (\*\*) for  $p < 0.05$  and (\*) for  $p < 0.10$ .

Note that, even though we collected three patterns per user (for the three different scenarios), we never use more than one in the comparison, as we test the results for each (fictive) scenario separately.

#### B. Results for the entire population

First, we report some results for the entire population.

*Pattern creation time.* The time required to complete a task is one fundamental aspect of the usability of an (authentication) system. We measured the pattern creation time from when the empty grid was displayed on the screen until the user submitted the pattern (separately for each scenario). Table III gives the median creation times for each of the three scenarios that we tested, both for the entire set of users as well as for the subsets of those who reported previous experience with AUP and those that reported no previous experience. (We use the median for its robustness to outliers, as we have encountered some outliers that presumably started the creation process, waited a while, and only returned to their device much later.)

The creation times differ with the (fictive) scenario; it is lowest for the smartphone unlock scenario (6.45 sec), middle for the shopping scenario (7.06 sec), and highest for the bank scenario (8.08 sec). All three differences are statistically significant (as a Mann-Whitney U-Tests show: Shopping vs. Smartphone  $p = 0.026736$ , Shopping vs. Bank  $p < 10^{-5}$ , Smartphone vs. Bank  $p < 10^{-12}$ .) This gives an indication that the (fictive) scenarios used in the study have actually influenced the participants. Also, this gives indication that users invest more effort for accounts with higher (perceived) security requirements, and we will see in the sequel that this increase in effort actually leads to patterns with higher strength.

Interestingly, we find no clear difference in creation times between participants that report experience with the Android Unlock Pattern scheme and those that report no experience. Both for the Shopping and the Bank subsets, we find no significant differences ( $p = 1$  in both cases), only in the

	Shopping	Smartphone	Bank	All
#Patterns	841	842	838	2521
Avg. Size	5.541	5.398	5.920	5.619
Avg. Length	5.050	4.920	5.666	5.212
Avg. # Intersections	0.210	0.1769	0.433	0.273
Avg. Overlaps	0.0178	0.014	0.023	0.018
Min.	2.16	2.16	2.16	2.16
1st Qu.	5.84	5.85	6.72	6.18
Median	7.98	8.16	9.35	8.42
Mean	8.86	8.88	10.40	9.37
3rd Qu.	11.12	11.17	13.11	11.72
Max.	32.11	33.19	34.82	34.82

TABLE IV. BASIC STATISTICS FOR THE PATTERN STRENGTH.

Smartphone scenario the difference is significant ( $p < 10^{-5}$ ). It is unclear to us why the smartphone scenario behaves differently than both other scenarios.

*Pattern strength.* Table IV shows the average and median strength of the patterns in the three sets that we collected, as well as several other statistics about the patterns. The (median) strength of the collected patterns differs for the different scenarios, even though they were purely fictional and no consequences followed from it. The strength of the patterns in the Bank scenario were significantly stronger than those in the Shopping scenario ( $p < 10^{-8}$ ) and those in the Smartphone scenario ( $p < 10^{-7}$ ), while there was no significant difference between the Shopping and Smartphone scenario ( $p = 1$ ).

*Bias of the patterns.* It has been demonstrated before (e.g. [26], [4], [7] and others) that patterns chosen by humans are biased. To facilitate comparisons with previous work we give some statistics about the structure of the observed patterns in the sequel.

Two aspects that can be used to observe this bias are the distribution of the starting point and the bias of the observed  $n$ -grams. The distribution of the starting point is shown in Figure 4(a). This distribution is similar to previously reported numbers: The top-left node is the most frequent one with 44% starting at this particular node (Uellenbeck et al.: 43%), followed by the top-right with 15% (Uellenbeck et al.: 9%) and bottom left with 14% (Uellenbeck et al.: 18%), the remaining nodes ranging from 2% to 9% (Uellenbeck et al.: 2% to 8%).

The most frequent 3-grams are shown in Figure 4(b), where the left figure shows the most frequent 3-grams. The similarities with previous work are striking and show a clear tendency to avoid the middle node, as well as selecting nodes with Euclidean distance one as next node.

A further source of bias is introduced by frequent patterns that resemble common symbols, specifically letters from the Latin alphabet. We inspected the dataset for occurrences of “letters”, and found that 385 out of 3393 patterns (11.4%) resembled a letter. Figure 4(c) shows the most frequent cases that we found in the dataset. The most frequent letters were three different versions of the letter “L”, as well as “Z”, “O”, “S”, and “U”.

### C. The influence of personal traits

Next, we present our main results on the influence of specific traits of the user on the resulting pattern strength. An overview can be found in Tables V and VI.

	1st Quart. / Median / 3rd Quart.			p	
Gender	Female		Male		
Shopping	5.30	7.66	10.18	5.85 8.15 11.83	0.1082
Smartphone	5.66	7.57	10.06	6.02 8.47 11.72	0.0204 (**)
Bank	6.47	8.50	11.38	6.89 9.79 13.42	0.0042 (**)
Handedness	Left		Right		
Shopping	5.28	7.66	10.55	6.07 8.10 11.39	0.8939
Smartphone	5.62	7.84	11.06	6.02 8.29 11.22	1
Bank	6.43	8.90	12.05	6.88 9.53 13.21	0.2570
IT experience	yes		no		
Shopping	5.85	8.15	11.65	5.48 7.66 10.27	0.1577
Smartphone	5.90	8.29	11.80	5.76 7.86 10.06	0.0725 (*)
Bank	6.92	9.43	13.14	6.46 9.09 12.57	0.3205

TABLE V. PATTERN STRENGTH FOR DIFFERENT SUBGROUPS.

	$\rho$	$p$
Age		
Shopping	-0.0803	0.1578
Smartphone	-0.0435	1
Bank	-0.1123	0.00986 (**)
Handsize		
Shopping	0.0175	1
Smartphone	0.0408	1
Bank	0.0264	1

TABLE VI. PATTERN STRENGTH FOR DIFFERENT SUBGROUPS.

*Gender.* We found that gender has a significant influence on the pattern strength in the categories Smartphone and Bank ( $p = 0.0204$  and  $p = 0.0042$ , respectively), where female participants chose weaker patterns. The influence in the Shopping scenario is not significant ( $p = 0.1082$ ) (see also Table V). Digging deeper, we see that this is at least in part explained by differences in the patterns length chosen by the participants: female participants choose significantly shorter patterns in the Shopping scenario ( $p = 0.0060$ ) and in the Bank scenario ( $p = 0.00072$ ), but not in the Smartphone scenario ( $p = 0.721$ ). Length is one of the more intuitive factors for pattern strength that should be accessible to a broad audience, but is obviously not the only one.

*Handedness.* We speculated that the handedness of a participant could have an influence on the chosen patterns, as certain points might be easier to reach than others. This could have an effect on the strength of the chosen patterns. However, we found no significant difference in pattern strength for both groups (see Table V).

*Experience with IT or IT Security.* We tested the influence of the (self-reported) experience in IT or IT Security on the pattern strength. We found no statistically significant differences, but we found a significant interest (with  $p = 0.0725$ ) for the Smartphone scenario.

This lack of a clear influence was contrary to our expectations and interesting on its own. To better understand this phenomenon, we also considered pattern length and number of intersections, both which are typically associated with stronger patterns. We found a significant influence of experience on the pattern length in the Banking scenario (Shopping:  $p = 0.206$ , Smartphone:  $p = 0.534$ ; Bank:  $p < 0.0001$ ), while there was no significant influence on the number of intersections (Shopping:  $p = 0.218$ , Smartphone:  $p = 0.269$ , Bank:  $p = 1$ ).

While we have no conclusive explanation for this behavior, it seems plausible that users with experience where trying to

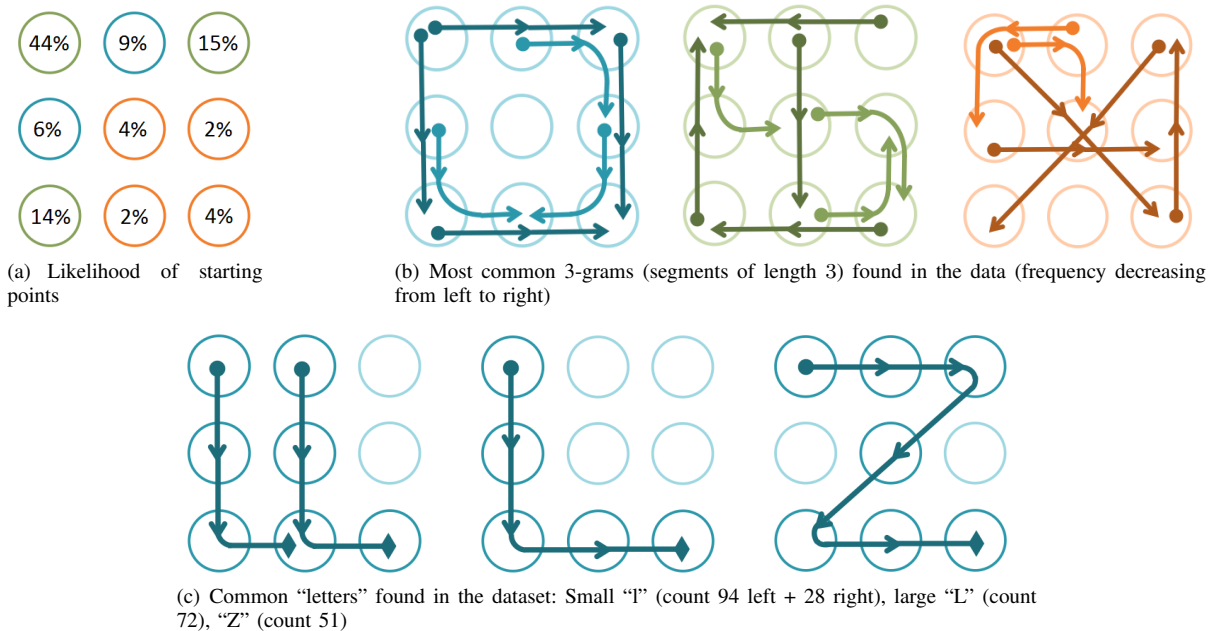


Fig. 4. Basic characteristics of the collected patterns.

choose stronger passwords, but failed in doing so (according to the used strength metric).

*Age.* The age of the participants has some influence on the strength of the patterns (see Table VI). While the correlation in the Shopping and Smartphone scenario was not significant, we found a significant correlation in the Bank scenario ( $p = 0.0264$ ). The correlation factor for the Bank scenario is moderate ( $\rho = -0.113$ ), i.e., older participants tend to choose weaker patterns. One likely explanation is younger people are generally more technology-affine and thus more used to such schemes.

*Handsize.* We assumed that a participant's handsize could influence how well she can draw certain complicated patterns (e.g., patterns including a "knight move"), given that mobile devices usually have a very limited screen-size. However, we found no significant correlation of the (self-reported) handsize on the strength of the chosen patterns (see Table VI).

## VI. DISCUSSION

Finally, we discuss some limitations and provide an outlook on future work.

### A. Limitations

As with all surveys, we rely on the people answering the questions truthfully, and selecting patterns that are realistic. Actually, as our main interest is in comparing strength of different subsets of our dataset, most of our results are invariant to a bias in pattern strength, as long as it affects all collected patterns the same.

As a consequence of our recruitment process via social networks and mailing lists, our participant set is biased towards young (62% are between 20 and 29 years) male (66%) students with a background in IT or IT security (59%) from Norway

(64%), thus it does not represent the overall population. As we have seen in Section V-C, specifically age and experience with IT or IT security do influence the pattern strength. However, in the actual comparison the influence of the biased sample should be small, as we are comparing across these subgroups.

### B. Future work

We have seen a clear influence of personal traits of a user on the pattern strength. One obvious question regards other measurable properties of users and their influence on pattern strength. Particularly interesting seems the participant's reading- and writing-direction, which we didn't test due to lack of participants with non-western reading-direction.

While in this work we were only concerned with discovering connections between the overall strength and personal traits, there are two directions for future work using these results. Motivated by these findings, one can construct statistical models for individual patterns of a single user, instead of considering the average strength only. Such models can be used first for helping users choose stronger patterns, taking into account their personality, and second for improving the guessing of patterns for the purpose of forensics.

Finally, it would be interesting to extend our findings to other authentication schemes. While some influencing factors are known (see Section II), we are still lacking a more systematic understanding of those factors.

## VII. CONCLUSION

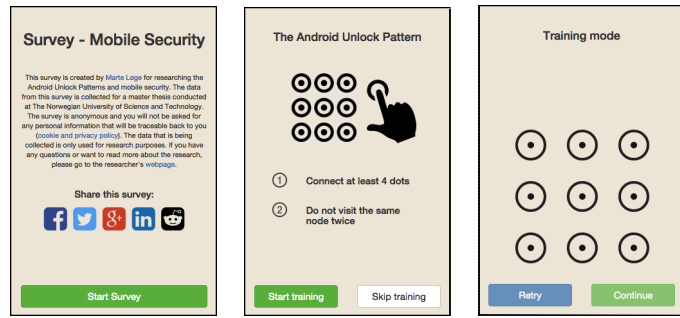
In this work we have shown that personal traits of a user influence the strength of patterns selected for the Android Unlock Patterns. Specifically we have found statistically significant differences in strength based on age and gender, as well several structural properties of patterns. We believe this work is a step towards a more personal treatment of (graphical)

password strength, with the potential to offer more useful password advice for users.

## REFERENCES

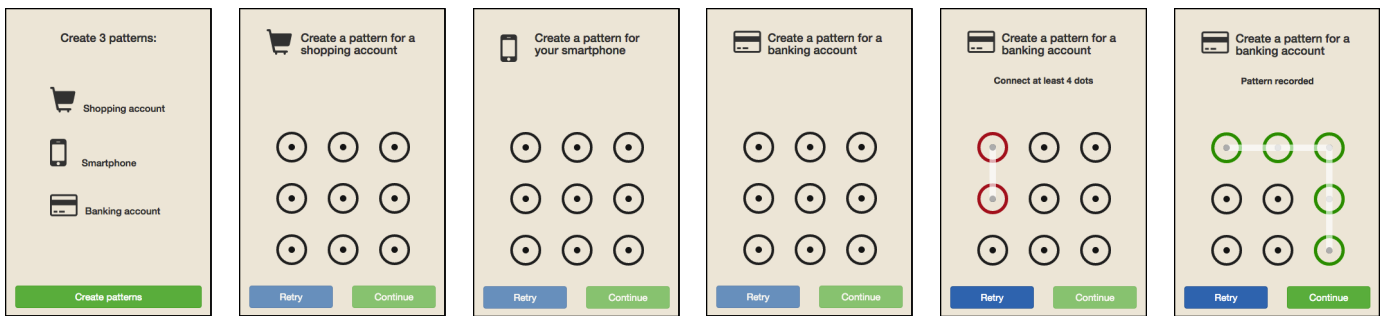
- [1] P. Andriotis, T. Tryfonas, and G. Oikonomou, "Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method," in *Proc. Human Aspects of Information Security, Privacy, and Trust*. Springer, 2014, pp. 115–126.
- [2] P. Andriotis, T. Tryfonas, G. Oikonomou, and C. Yildiz, "A pilot study on the security of pattern screen-lock methods and soft side channel attacks," in *Proc. ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2013, pp. 1–6.
- [3] M. Arianezhad, D. Stebila, and B. Mozaffari, "Usability and security of gazebased graphical grid passwords," in *Proc. Financial Cryptography and Data Security Workshop on Usable Security (USEC)*. Springer, 2013, pp. 17–33.
- [4] A. J. Aviv, D. Budzitowski, and R. Kuber, "Is bigger better? comparing user-generated passwords on 3x3 vs. 4x4 grid sizes for android's pattern unlock," in *Proc. Annual Computer Security Applications Conference (ACSAC)*, 2015.
- [5] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in *Proc. Workshop on Offensive Technology (WOOT)*, 2010.
- [6] A. J. Aviv, B. Sapp, M. Blaze, and J. M. Smith, "Practicality of accelerometer side channels on smartphones," in *Proc. Annual Computer Security Applications Conference (ACSAC)*, 2012.
- [7] A. J. Aviv, J. Maguire, and J. L. Prak, "Analyzing the impact of collection methods and demographics for android's pattern unlock," in *Proc. Workshop on Usable Security (USEC)*. Internet Society, 2016.
- [8] G. Blonder, "Graphical password," 1996, US Patent 5559961.
- [9] J. Bonneau, "The science of guessing: Analyzing an anonymized corpus of 70 million passwords," in *Proc. IEEE Symposium on Security and Privacy (SP)*, 2012, pp. 538–552.
- [10] J. Bonneau, S. Preibusch, and R. Anderson, "A birthday present every eleven wallets? The security of customer-chosen banking PINs," in *Proc. Financial Cryptography and Data Security*. Springer, 2012, pp. 25–40.
- [11] C. Castelluccia, C. Abdelberi, M. Dürmuth, and D. Perito, "When privacy meets security: Leveraging personal information for password cracking," *CoRR*, vol. abs/1304.6584, 2013. [Online]. Available: <http://arxiv.org/abs/1304.6584>
- [12] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in *Proc. USENIX Security Symposium*. Usenix, 2004.
- [13] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," *Int. J. Hum.-Comput. Stud.*, vol. 63, no. 1-2, pp. 128–152, Jul. 2005.
- [14] A. E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the PassPoints graphical password scheme," in *Proc. Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2007, pp. 20–28.
- [15] P. Dunphy and J. Yan, "Do background images improve draw a secret graphical passwords?" in *Proc. ACM Conference on Computer and Communications Security (CCS)*. ACM, 2007.
- [16] S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner, "Are you ready to lock?" in *Proc. ACM Conference on Computer and Communications Security (CCS)*. ACM, 2014.
- [17] M. Harbach, E. von Zezschwitz, A. Fichtner, A. D. Luca, and M. Smith, "It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception," in *Proc. Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, 2014.
- [18] C. Hardyck and L. F. Petrino, "Left-handedness," *Psychol. Bull.*, vol. 84, no. 3, pp. 385–404, may 1977.
- [19] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in *Proc. USENIX Security Symposium*, 1999.
- [20] D. V. Klein, "Foiling the cracker: A survey of, and improvements to, password security," *Proc. USENIX Security Workshop*, 1990.
- [21] Y. Song, G. Cho, S. Oh, H. Kim, and J. H. Huh, "On the effectiveness of pattern lock strength meters: Measuring the strength of real world pattern locks," in *Proc. Annual ACM Conference on Human Factors in Computing Systems (CHI)*, 2015.
- [22] C. Sun, Y. Wang, and J. Zheng, "Dissecting pattern unlock: The effect of pattern strength meter on pattern selection," *Journal of Information Security and Applications*, vol. 19, no. 4–5, pp. 308–320, Nov. 2014.
- [23] H. Tao and C. Adams, "Pass-Go: A Proposal to Improve the Usability of Graphical Passwords," *International Journal of Network Security*, vol. 7, no. 2, pp. 273–292, 2008.
- [24] J. Thorpe and P. C. Van, "Graphical dictionaries and the memorable space of graphical passwords," in *Proc. USENIX Security Symposium*. Usenix, 2004.
- [25] —, "Human-Seeded attacks and exploiting Hot-Spots in graphical passwords," in *Proc. USENIX Security Symposium*. Usenix, 2007.
- [26] S. Uellenbeck, M. Dürmuth, C. Wolf, and T. Holz, "Quantifying the security of graphical passwords: The case of android unlock patterns," in *Proc. ACM Conference on Computer & Communications Security (CCS)*. ACM, 2013, pp. 161–172.
- [27] D. Van Bruggen, S. Liu, M. Kajzer, A. Striegel, C. R. Crowell, and J. D'Arcy, "Modifying smartphone user locking behavior," in *Proc. Ninth Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2013.
- [28] E. von Zezschwitz, P. Dunphy, and A. D. Luca, "Patterns in the wild: A field study of the usability of pattern and pin-based authentication on mobile devices," in *Proc. International Conference on Human-computer Interaction with Mobile Devices and Services (MobileHCI)*, 2013.
- [29] S. Wiedenbeck, J.-C. Birget, A. B. J. Waters, and N. Memon, "Authentication using graphical passwords: Basic results," in *Proc. International Conference on Human-Computer Interaction (HCI International)*, 2005.
- [30] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: effects of tolerance and image choice," in *Proc. Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2005, pp. 1–12.
- [31] —, "PassPoints: Design and longitudinal evaluation of a graphical password system," *Int. J. Hum. Comput. Stud.*, vol. 63, no. 1-2, pp. 102–127, Jul. 2005.
- [32] Z. Zhao, G.-J. Ahn, J.-J. Seo, and H. Hu, "On the security of picture gesture authentication," in *Proc. USENIX Security Symposium*, 2013.

## APPENDIX

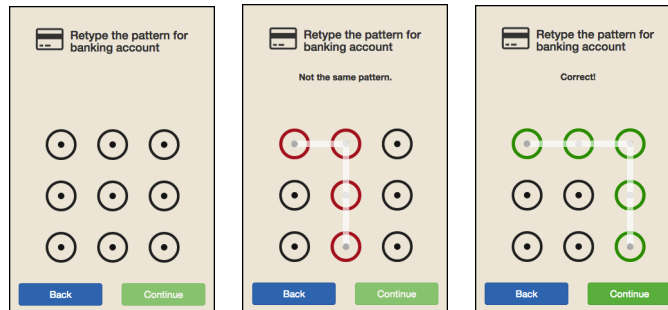


(a) Start screen      (b) Android Unlock Pattern introduction      (c) Training mode (optional)

Fig. 5. Study design – Introduction



(a) Introduction to patterns      (b) Shopping pattern      (c) Smartphone pattern      (d) Bank pattern      (e) Pattern length too short      (f) Valid pattern recorded



(g) Retype pattern      (h) Retype wrong      (i) Retype correct

Fig. 6. Study design – Create and retype patterns

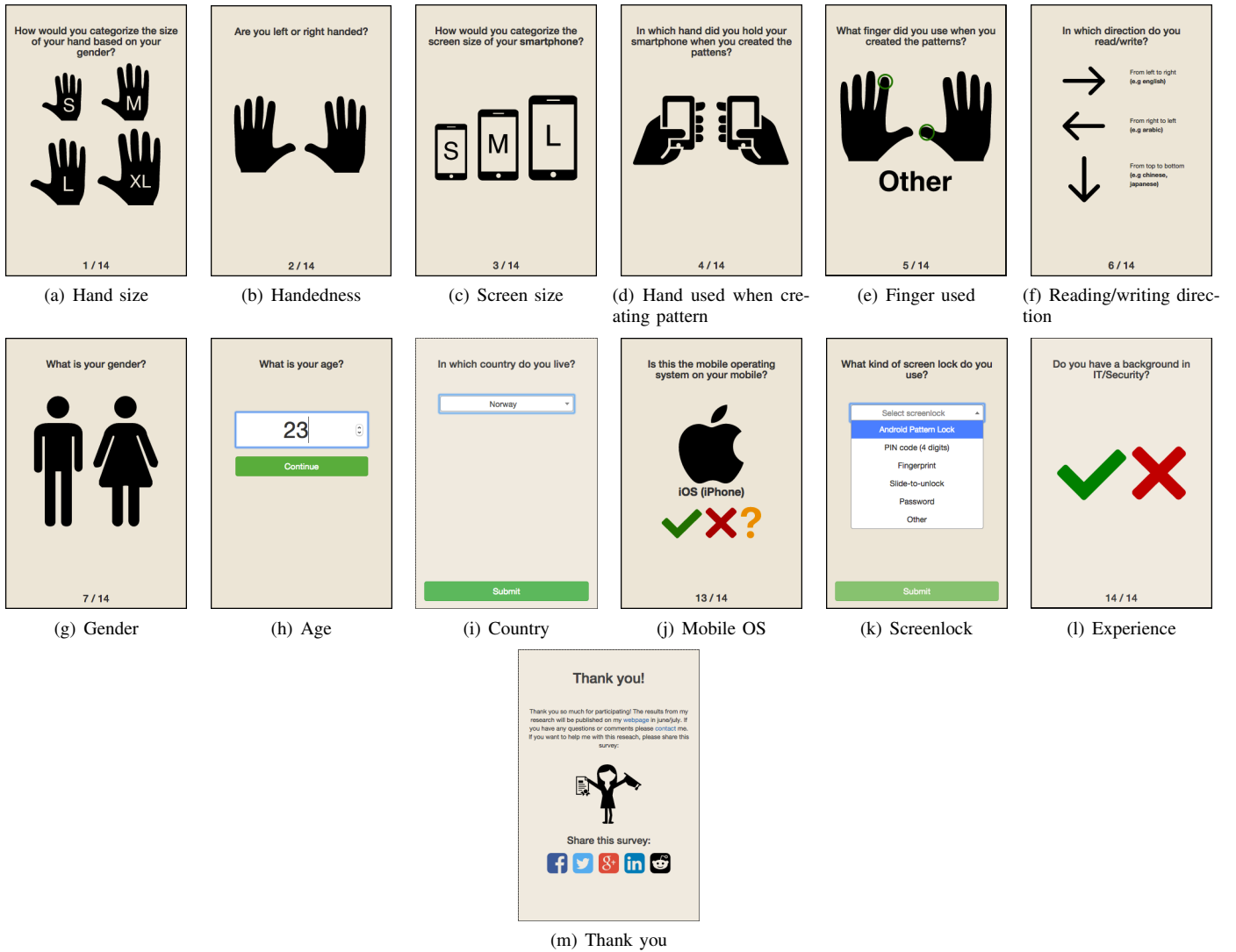


Fig. 7. Study design – Demographic questions



# Influencing Self-Selected Passwords Through Suggestions and the Decoy Effect

Tobias Seitz, Emanuel von Zezschwitz, Stefanie Meitner, Heinrich Hussmann  
Media Informatics Group

LMU Munich

Email: tobias.seitz@ifi.lmu.de, emanuel.von.zezschwitz@ifi.lmu.de,  
meitner@cip.ifi.lmu.de, hussmann@ifi.lmu.de

**Abstract**—We present results from an online experiment with the goal of nudging users towards stronger passwords. We explored the effect of suggesting different variations and constellations of passwords during password selection. In particular, we investigated whether the *decoy effect* can be applied here: When people face a choice between two options, adding a third, unfavorable option can influence their decision making process. As a usage scenario, we constructed a choice architecture for password generators that followed this decoy pattern and compared their effect regarding usability and security. While a previous study indicated positive results, we received mixed results regarding the feasibility of the decoy effect. Based on our study, we can however propose concepts to improve persuasive approaches to nudge users towards stronger password strategies.

## I. INTRODUCTION

*“Making decisions is like speaking prose – people do it all the time, knowingly or unknowingly.”* [1]

This quote by Kahneman and Tversky puts our daily decision making tasks into a nutshell. Decisions can be enjoyable, if they give people a sense of autonomy and control. On the other hand, having to decide is often difficult and arduous. To simplify the task, people use certain rules of thumb – knowingly or unknowingly [1]. Here, *framing effects* can impact people’s heuristics. A prominent example that surrounds us in daily life when we buy goods is the decoy effect. It is a marketing phenomenon where the deliberate introduction of an unfavorable option makes higher priced options more attractive [2]. Customers usually compare the goods instead of looking at them individually. With this heuristic, they often accomplish to rule out an unfavorable option, namely the decoy, or they can determine their priorities.

Our aim in this work is to exploit this effect to influence the decision making process during password selection. Choosing and maintaining a password is onerous for users because it creates overhead to their primary task of actually using a system [3]. There have been many propositions to ameliorate the process for them, e.g. by providing real-time feedback on the entered password [4] or by suggesting a suitable secret [5].

Permission to freely reproduce all or part of this paper for noncommercial purposes is granted provided that copies bear this notice and the full citation on the first page. Reproduction for commercial purposes is strictly prohibited without the prior written consent of the Internet Society, the first-named author (for reproduction of an entire paper only), and the author’s employer if the paper was prepared within the scope of employment.  
EuroUSEC ’16, 18 July 2016, Darmstadt, Germany  
Copyright 2016 Internet Society, ISBN 1-891562-45-2  
<http://dx.doi.org/10.14722/eurousec.2016.23002>

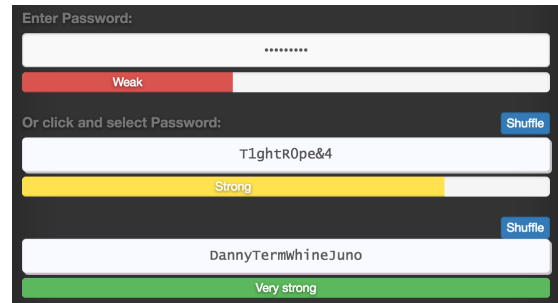


Fig. 1. The Decoy Password Generator evaluates and suggests passwords. The first suggested password is the ‘decoy’, which is difficult to type and not optimally strong. The second is the ‘target’, an easy to type and supposedly easy to remember password.

The latter approach can be highly beneficial in terms of security but often shows usability drawbacks.

As use-case for the decoy effect, we investigated if giving the user a choice between generated passwords increases involvement and improves password strength metrics. Instead of suggesting just one password at a time, we add another option that serves as a decoy, i.e. it is an unfavorable option and should make a better option stand out and more attractive. This choice architecture was expected to nudge users to make a more favorable decision in terms of usability and security.

In summary, we contribute empirical evidence from an online experiment that investigated (a) the existence of the decoy effect for password selection and (b) the feasibility of password suggestion to influence self selected passwords. We (c) present a password generator concept that nudges users towards stronger passwords and (d) we discuss implications for further utilization. Even though the decoy effect did not show the expected results, we learned that directly comparing one’s own password to a generated strong alternative can have a positive impact on the strength of self-selected passwords.

## II. BACKGROUND AND RELATED WORK

The decoy effect is a popular tool in the framing of options, which inspired us to exploit it when people pick passwords. Applying it in this context, we motivate the comparison of passphrases to seemingly more complex passwords to produce the effect. Furthermore, we shed light on non-verbal persuasion which is our ultimate goal in this work.

### A. The Decoy Effect

The decoy effect “shifts people’s reference points” as Lockton puts it [6]. This effect, which is also known as the asymmetric dominance effect [2], comes into play when people face a choice between three items that can be ranked on two dimensions, for example quality and effort. The items are labeled **competitor**, **target** and **decoy**. The competitor usually is an inexpensive option with low quality. The target is the one item that vendors are trying to sell. It is more expensive, but its quality is superior to the competitor’s. Finally, the decoy is an unfavorable, or even irrational option for the buyer as it is more expensive than but not as good as the target. Depending on the presence of the decoy option, a person’s preference for one of the alternatives can be influenced.

The decoy can be constructed in numerous ways by varying its values along the two dimensions, e.g. price and quality, as described in [2]. Reasoning about the origin, Ariely and Wallsten provide evidence that people actively seek ways to simplify the task [7]. To accomplish this, they employ heuristics or “rules of thumb”. Customers compare the options and relate each item to the others. The decoy evidently influences this comparison. Directing people’s choices like that is sometimes termed “choice architecture” [8], [9] and has recently become a topic for usable security and privacy (e.g. [10], [11], [12], [13]).

### B. Passphrases and High Complexity

The decoy effect requires alternatives to be easily comparable in the most obvious dimensions. Therefore, we explored password composition strategies facilitating comparison for humans regarding “**strength**” and “**complexity**”.

A first composition strategy are passphrases based on a number of dictionary words. Shay et al. investigated system assigned passphrases consisting of common words [14]. On usability scales, passphrases performed similarly to more complex, but shorter passwords. In another study they examined security and usability of password creation under different password policies [15]. They concluded that a policy requiring two separate words with a total length of 16 characters (2word16) can outperform more complex policies requiring fewer characters (comp8 or 3class12). In terms of passphrase usability, research is contentious. On the one hand, Shay et al.’s evidence indicates nearly equal performance [14], [15]. On the other hand, Keith et al. showed that users’ perception and ability to memorize passphrases largely depend on the construction of a passphrase [16]. If the passphrase chunks were separated by delimiters that appear in regular text processing, users perceived such a strategy as enjoyable.

In summary, random password strings and passphrases seem to perform almost equally in terms of usability and security. However, we assumed that word-based passphrases would simplify the assessment of different complexity levels as the chunks are more easily identifiable [16]. This makes them stand out against complex character strings and therefore suitable for the decoy effect.

### C. Non-Verbal Persuasion for Stronger Passwords

Nudging users towards stronger passwords has been under constant research for years. For example, proactive password meters are well established and provide visual, non-verbal information about the entered password [4]. They are effective because they can persuade users to try and achieve a high “score”. Apart from the issue that the feedback provided is highly inconsistent across different services [17], it was also found that the way users try and increase their score is predictable [18]. A common strategy is to add numbers and/or an exclamation mark at the end. We also use password meters in our concept (cf. Section III). Users can compare the strength of their self-chosen password to at least one alternative. We hypothesize that instead of just adding a digit at the end of their re-used password, users might consider inserting an entire word or substitute a letter after seeing an example passphrase constructed in this way.

Finally, we consider password suggestions *persuasive*. After Fogg coined the term persuasive technology [19], Weirich and Sasse were probably the first ones to put forward the understanding that users could also be persuaded to alter their password behavior [3]. Like us, Forget et al. [20], [21]. utilized suggestions to improve users’ passwords. However, their approach was denoted by modifying the users’ existing passwords. They found that suggestions are effective in increasing password strengths in regard to cracking attacks.

## III. DESIGN-CASE: THE DECOY PASSWORD GENERATOR

Our “Decoy Password Generator” suggests two passwords at once: One long passphrase with low complexity and one short password with high complexity. The latter, contrary to intuition, has a lower quality ranking than the first because its letter substitutions are predictable to some degree. The result is expected to create an asymmetric dominance effect. The concept presented here is the result of an online survey [22] and an online experiment which we describe in the subsequent sections. As discussed below, this use-case produced a different result than we anticipated but still provided valuable insights into the attractiveness of generated passwords.

### A. Choice Architecture

**Offer alternatives.** The generator suggests two different passwords to increase the users’ level of autonomy and to incentivize comparison. Offering multiple options allows the users to consider different, potentially stronger options than what they would usually come up with. We construct the suggestions in a decoy pattern and show password meters beneath to display their quality. Ideally, users are nudged towards an optimal choice in terms of effort and strength. The user is not required to pick between their own password and a suggestion. Rather, the suggestions serve as a good example.

**The competitor is the users’ own password.** We consider the users’ self-selected password as competitor. We expect it to rank low on both the “effort” and the “quality” scale.

**The target consists of dictionary words.** The suggested password is a passphrase similar to what Shay et al. studied

in [14]. Combining four words yields high-entropy passphrases (see Section III-B) that can cope well with offline attacks [15]. We capitalize the words mainly for readability reasons. This kind of passphrase makes for a very strong password, whose chunks are easily identifiable but requires some effort to type and memorize.

**The decoy is shorter, but complex.** This suggestion looks more complex because it is a mangled word, followed by two random characters. The result is a password that has 4 character classes and is at least 10 characters long. The resulting password is not optimal, because password cracking tools can cope with this kind of mangling if they are well-configured [15].

One could argue that an increase in available options goes along with a more complicated decision. Indeed, there is evidence for a choice proliferation dilemma [13], [23], and the results of our online experiment also point in this direction. On the other hand, offering choice presumably gives a higher degree of autonomy, which in turn can be a strong motivator according to the self-determination theory of motivation [24]. Thus, having more options to choose from might actually result in people making the choice instead of skipping the suggested passphrases. Still, it is required that the suggestions be constructed perfectly to produce this effect.

Furthermore, making people adhere to a certain password policy reflects badly on the user experience [25]. The more complicated the requirements the more annoyed users become. Another effect of imposing heavy restrictions is that users try and get away with the simplest password meeting the requirements [18], and therefore may even result in a decrease of overall strength. Thus, it seems vital for the user experience to find ways to move away from restrictive password policies. The suggested passphrases from our generator can adhere to an underlying policy without the users even noticing it.

## B. Implementation

Many password generators only create one password at a time and users can afterwards regenerate it, if necessary. To examine the decoy effect, we construct two random alternatives that follow our choice architecture:

Generated password	Strength
(A) DennyTermWhineJuno	(very strong)
(B) T1ghtR0pe&4	(strong)

For option (A), each word is chosen randomly from the Diceware dictionary<sup>1</sup> of 5823 words, including short words that most of us usually do not actively use, e.g. *girth*, *infix*, *thine*. With a minimum word length of three and a maximum of five characters, we generated passphrases between 12 and 20 characters. The resulting password space is  $5823^4 = 1149706959914241 \approx 10^{15}$ . The entropy of one word is  $(\log_2(5823) \approx 12 \text{ bits})$ , and the entropy of the entire password is approximately  $(2^{12})^4 = 48 \text{ bits}$ .

<sup>1</sup><http://world.std.com/~reinhold/diceware.wordlist.asc>, last access on April 29th 2016

For option (B), the generator randomly selects a word from a 687 word subset of the dictionary. The words have to be at least 8 characters long. Then the word is mangled and extended by two random characters, resulting in a password that has 4 character classes and is at least 10 characters long. The decoy passwords have  $\log_2(687) \approx 9$  bits of entropy in the basic form. The entropy increases with capitalization (1 bit), one uppercase letter (2 bits), two common substitutions (2 bits), punctuation (4 bits), and finally with the number added at the end (3 bits). The total entropy is thus 21 bits, if an attacker knows exactly which subset from the dictionary was used.

Marketing psychology research has also investigated explanations for the effect and concluded that offering clear reference points to reduce the difficulty of comparisons is a key factor here [7]. The strength ratings and password meters are reference points in our setting. If we transfer this argumentation to our scenario, we see that despite the complexity of the decoy-option (B), the outcome is weaker than the target-option (A). We therefore expect users to prefer option (A).

For the remainder of the paper, we refer to the target option (A) as the *passphrase* and to the decoy option (B) as the *mangled password*.

## IV. RESEARCH GOALS

To the best of our knowledge, research on the impact of showing generated passwords during password selection on the final selection is rare. Since empirical evidence about the existence of the decoy effect in the realm of passwords is missing, our goal was to collect such evidence. We thus posed the following research questions (RQ):

**RQ1:** Is there a quantitatively measurable effect on self-selected passwords after receiving password suggestions? If there is, what do the suggestions have to look like?

**RQ2:** Do users create stronger passwords if they receive two suggestions in a decoy pattern instead of just one random password?

**RQ3:** To what degree is memorability affected by displaying password suggestions?

## V. ONLINE EXPERIMENT

We utilized a crowd-sourced study tool<sup>2</sup> to get responses from a heterogeneous sample. Given that this kind of study is thoroughly planned, the methodology has been shown to deliver reliable results in many password studies before (e.g. [14], [17], [18], [26]).

### A. Goals

We first isolated the passphrase and the mangled password to compare their influence separately (RQ1). This would allow more detailed insights into the nature of a suggested password. We also aimed to show that multiple suggestions have a greater impact on password selection than single suggestions (RQ2). Last, we also intended to measure the memorability of the passwords (RQ3). System-assigned passwords are usually less

<sup>2</sup><http://prolific.ac>, last access on May 8th 2016

easy to remember [14], which is why this factor is important regarding the usability of such nudging approaches.

## B. Methodology

The study was conducted online in a between groups design with four conditions: The **Control Group** did not receive password suggestions. The second group only saw one suggestion and was divided into two sub-groups: only the four-word passphrase was generated in the **Words** condition, while a mangled password was shown in the **Mangled** condition. Finally, the password generator delivered both the passphrase and the mangled password in the **Decoy** condition.

1) *Study Procedure*: The study was split into two parts. The first part included the password selection and first usability assessment through a questionnaire. The second part was carried out three days after the first to measure memorability and collect further qualitative feedback. We created a web page containing an introduction, a password-selection task and a questionnaire. The introductory part constructed the scenario: The website asked participants to imagine they were creating a new password for their main email account. For the first part, valid responses were reimbursed with \$1.30. In the second part, respondents received another \$0.56 for a valid response. We rejected responses from participants whose completion times deviated from the mean more than three times the standard deviation, i.e the outliers.

2) *Measurements*: We decided not to collect passwords in plain text, because the nature of the study required that passwords could be linked back to the participants' email addresses. Therefore, we created meta statistics about the passwords (similar to [27]). For this purpose, we utilized the zxcvbn<sup>3</sup> password strength estimation library and extended it for our purposes. Zxcvbn bases part of the estimation on frequency lists and adjacency graphs. Hence, its scoring is especially reliable, because it takes mangling rules and common passwords into account beside dictionary entries [28]. The most important metrics in our study about the passwords were length, composition topology, strength rating on a scale from 0 (weakest) to 4 (strongest), and estimated guesses required to crack the password.

3) *Prototype*: Our prototype was a web-based application implemented with PHP and JavaScript. Passwords were generated and served via a PHP script. The application displayed a masked password field, the suggestions for the experimental groups, a password confirmation field and a submit button. Figure 1 shows a screenshot of the user interface. User input and password metrics were logged via JavaScript and the zxcvbn library. A server script received the data and stored it into a MySQL database.

Participants could click the password suggestions to transfer them to the password field. However, they needed to enter the password manually at least once when they were prompted to confirm their password. Consequently, we prohibited the option to copy and paste the passwords. Furthermore, the

passwords were scored by estimating the guessability using the zxcvbn algorithm. To provide instant feedback to the participants, the password field and also the suggestions were accompanied by an animated password meter relying on the zxcvbn strength metric. The strength meter was an animated progress bar and visualized five different scores: very weak, weak, ok, strong, very strong.

In a first informal pilot run of the study (N=12), we found that capitalizing the four words made them more readable and appealing (e.g. “DannyTermWhineJuno” instead of “dannytermwhinejuno”). In another pre-test (N=5), participants criticized the selection or constellation of words. We hoped to alleviate the problem by supplying a ‘shuffle’ button to allow the participants to regenerate a suggestion, in case they simply did not like the combination of words.

4) *Hypotheses*: We formulated the following hypotheses:

**H1a**: If the 4-word passphrase is suggested, the users create longer and stronger passwords, even if they do not accept the suggestion.

**H1b**: If the mangled password is suggested, users diversify their selection in terms of character classes.

**H2**: If both the passphrase and the mangled password are suggested, the positive effect on strength is bigger than with a single suggestion.

**H3**: If the chunks in the suggestion are easily identifiable, its memorability is improved.

5) *Sample and Demography*: We recruited participants through the crowd study platform Prolific. We required participants to be located in either the UK or US, to be at least 18 years old and have a successful survey completion rate of 95% or more. The resulting participant pool included around 10000 possible Prolific users.

106 respondents started the study. The responses of 7 participants had to be rejected because the completion code was either missing or erroneous, data was missing from the questionnaire or because the completion time was an outlier. The remaining 99 participants were invited to come back for the second part of the study, which 97 people did. However, 7 responses were incomplete and 7 were rejected for the same reasons as for the first part. The resulting N for our analyses is  $N = 83$  valid, and complete responses in both parts. The Control group was formed by  $n = 18$ , Words by  $n = 24$ , Mangled by  $n = 21$  and Decoy by  $n = 20$ . Participants were 30 years in average ( $SD = 10$ ) with 42% female. The majority of 78% was employed, 12% were students, 10% were unemployed. In average, our participants had 9 online accounts that they regularly log in to ( $SD = 5.6$ ), which tells us that they were in the relevant user group.

## C. Results

Our data was non-parametric in all dimensions. Consequently, for statistical testing, we used Kruskal-Wallis tests for numerical and chi-squared tests for categorical data. All follow-up analysis was done with Bonferroni corrected Mann-Whitney tests. We report statistics on a significance level of  $\alpha = 0.05$ .

<sup>3</sup><https://github.com/dropbox/zxcvbn>, last access on April 28th 2016

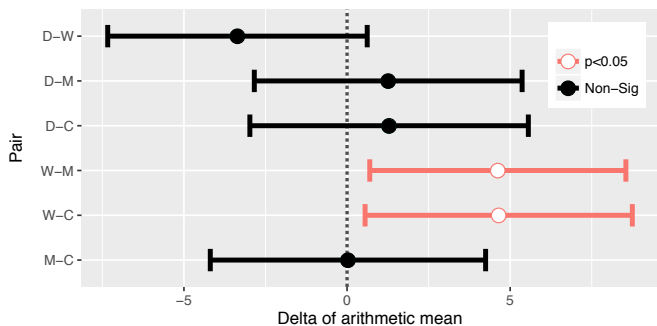


Fig. 2. Confidence intervals for pairwise comparisons of estimated guesses (log10). The plot indicates that users in the Words condition chose significantly stronger passwords than those in the Mangled and Control condition. (C = Control, W = Words, M = Mangled, D = Decoy.)

1) *Acceptance of Suggestions*: Overall,  $n = 9$  users accepted a suggestion (4 in the Words condition, 2 from Mangled, 3 from Decoy). In the Decoy condition, where both alternatives were visible, the passphrase was chosen twice and the mangled password once. We observed that 18 of 65 participants (27%) in the Words, Mangled, and Decoy conditions would have benefited from accepting a suggestion, i.e. their score was below 3 and would have been improved. The passwords of the rest were already ranked as “strong” in 23 and “very strong” in 24 cases. This indicates that the majority of the users rationally rejected the suggestions, because they would not have produced stronger passwords, while demanding a higher effort.

2) *Impact on Password Metrics*: The means and standard deviations on the most important metrics are shown in Table I. The confidence intervals of pairwise comparisons show that the estimated number of guesses required to crack the entered passwords is different in three conditions (see Figure 2). Using Bonferroni corrected Mann-Whitney tests, we confirm that participants in the Words condition selected significantly stronger passwords compared to the Control group ( $U = 128, r = -0.35, CI_{Words-Control}(\log) = [0.55, 8.74]$ ). Moreover, those participants in the Words condition who did not follow the suggestion still chose passwords that were about two characters longer in average compared to the control group ( $M_{Control} = 11.33 (SD_{Control} = 3.53), M_{Words} = 13.1 (SD_{Words} = 3.68, CI_{Words-Control} = [-0.9, 4.43])$ ).

3) *Password Topology & Policy Adherence*: We categorized compositions of each password to make them more comparable to policies put forward in e.g. [15]. The result is shown in Table II in the appendix. A chi-squared test did not reveal significant differences across groups ( $\chi^2(18) = 16.93, p > 0.5$ ). Nonetheless, the data shows that even though we followed a rather weak basic8 policy, all our participants used at least two character classes in their passwords. The majority (78%) even used three character classes. Participants in the Mangled condition were twice as likely to create passwords following the more challenging policies (comp8, 3class12, 3class16) than the control group. In average, the length requirement was exceeded by 4 characters.

4) *Memorability*: After three days,  $n = 34$  (40%) participants of the first part of the study succeeded to enter the previously chosen password. A chi-squared test did not reveal significant differences across groups ( $\chi^2(3) = 3.84, p > 0.05$ ). In the questionnaire, 76% of successful participants ( $n = 26$ ) reported to have entered the password from memory, while the rest either stored it in their browser (2), in an external file (5) or wrote it on paper (1). Those who accepted a suggestion performed poorly in terms of memorability. Only one participant of the Decoy group correctly entered the mangled password in the second part, reportedly from memory.

5) *General Qualitative Findings & Feedback*: We also collected qualitative feedback and ratings on 5-point rating scales in the questionnaires. The data was homogeneous across groups, so we report overall frequency distributions.

We asked participants in all the experimental groups, what their first reaction was to the suggestions. They could select multiple options from a list and provide additional text. The most clicked reactions were “neutral” ( $n = 25$ ), “surprised” ( $n = 23$ ) and “pleased” ( $n = 11$ ). When asked whether the suggested passwords would make their own email accounts more secure, we received a normally distributed vote on the 5-point scale ranging from “strongly agree” to “strongly disagree”. 20 participants (24%) agreed to the statement that they would be annoyed if their main email provider suggested a password like the one in the study. Still, 30 people (36%) agreed that it would make creating a password for an email account easier. 36 (43%) indicated that they preferred having a password with personal meaning.

## VI. DISCUSSION AND IMPLICATIONS

From our results we derive a set of implications for the practical application of advanced password suggestion.

### A. Even Rejected Suggestions can Improve Passwords

Although most suggestions were rejected, the passphrase had a positive impact, which we see as evidence for **H1a**. We primarily explain the rejection of suggested passwords with the high overall scores of the self-selected passwords. This made it unnecessary for many participants to figure out why the mangled word was marked as “strong”. The Decoy group may have rejected the suggestion because the strength label of the mangled password contradicted the strength of the passphrase too much. Participants were possibly confused and could not explain why the mangled password was rated worse, and so they continued with their own password. The suggestions could also have been rejected, because there was no actual benefit of using them during the study. Suggestions could prove more useful if they give feed-forward and make the benefit of using a stronger password more graspable to the users. For instance, suggestions can be accompanied by a benefit like infinite expiration dates.

### B. Strength Indication Facilitates Comparison

While the results indicate that the nudging power of the strength indicators is limited, we argue that it allows easy

comparison of the provided options. A password generator showing a passphrase marked as “very strong” lead participants in our study to choose longer and stronger passwords than those of the groups where the long passphrase was missing. This again speaks in favor of **H1a**. Thus, comparing the strength of the suggestion to a self-selected password apparently helps monitoring the strength more than only displaying a password meter. We suggest registration pages to react to weak passwords and display a randomly generated suggestion. Thereby, users can compare and improve their self selected password – and sometimes they might accept the entire suggestion, as we observed with 13% of participants.

### C. Suggestions Only for Those Who Need it

The results illustrate that users are unlikely to accept a suggested password if their own selection scores high already. In all four groups, the estimated number of guesses is more than  $10^8$ , which lies beyond the proposed threshold of a “resource-limited attacker” [15]. Interestingly, the cut-off threshold for exhaustive attacks ( $10^{12}$ ) was only achieved in the group where the passphrase was suggested. In addition, we saw that most self-selected passwords largely exceeded our basic8 policy. This partially supports **H1b**, but the evidence is not sufficient at this point. Those participants who included at least three character classes probably have been told in the past that this is necessary to compose a strong password. Therefore, we conclude that the rejection of the suggestions was partly due to many participants already opting for a strong self-selected password, as they had little to no room for improvement through accepting the suggestion. We propose adjusting the suggestion strategy depending on the user’s initial self-selected password. For instance, one could only display suggestions until the password has reached a certain strength.

### D. Multiple Password Suggestions are Unfeasible

When *both* the passphrase and mangled password were suggested, the strength of the self-selected passwords slightly increased, but the length did not. Therefore, we reject **H2** and conclude that it is probably unfeasible to suggest multiple passwords side by side in a decoy choice architecture. The memorability results as well as qualitative feedback indicate that acceptance might have been reduced by the composition style of the suggestions which included many uncommon words (**H3**). While the option to re-generate suggestions was used by 6 participants, none of them were satisfied with the results and none of the suggestions was finally accepted. Overall, the decoy effect was rather ineffective and participants were persuaded to a higher degree, if only one suggestion was shown. Here, the passphrase generated the highest measurable impact. We argue that system-*suggested* passwords should therefore be based on one option which is long enough, but not necessarily highly complex. System-assigned passwords, on the other hand, could be shown in a decoy pattern to make the users feel a little happier about the assignment. They can at least choose and have some degree of autonomy [24], which might improve user experience.

## VII. LIMITATIONS

Our password study, like others, has limitations. First, we screened participants such that only those with a successful study record could participate, so the resulting passwords might not be representative for the entire population. Since our password policy requirements were exceeded by far and the participants’ self-assessment indicated high effort, we believe that the real-world passwords are weaker. Leaked password databases highlight this [26]. Hence, such strong passwords make it difficult for us to nudge users towards even stronger passwords. Nonetheless, we succeeded with our target password, i.e. a passphrase.

The strength estimation that we utilized is inherently less robust than a more complex password guessing approach, like PGS<sup>4</sup> at Carnegie Mellon University [29]. However, it is one of the most reliable options [28] if one cannot collect plain text passwords as was the case in our study setting.

## VIII. CONCLUSION AND FUTURE WORK

We presented the influence of different password suggestions on the strength of self-selected passwords. Suggestions were accompanied by a quality indicator and either composed of four dictionary words or a short, complexly mangled word with additional characters. As previous work pointed in this direction, we hypothesized that showing multiple generated passwords at once would nudge users to accept the target suggestion. This was not the case in this experiment (RQ2). The four-word passphrase produced the highest impact on the strength of the passwords selected in our study. Participants who were only suggested the passphrase chose significantly stronger passwords. Thus, nudging users towards a stronger password apparently is more effective if a long, not necessarily complex password is suggested next to the password input field. Showing a more complex password only marginally increased the complexity of the selected passwords (RQ1). Our effective sample size was too small to draw conclusions on the nuances of memorability differences of our password suggestions (RQ3). Future research should investigate additional qualities of password suggestions. Basing suggestions on a user’s composition strategy might make them more attractive and effective. Offering a graspable benefit with suggestions might succeed in persuading users. We will evaluate this and other strategies by deploying production-ready systems at different web services. This will also allow us to collect data in the field and address the limitations of our studies.

In conclusion, we argue that it is feasible to learn from other scientific areas, in our case consumer psychology and behavioral economics, to inspire concepts in usable security [11], [30]. Yet, password selection is not the only use case for the decoy effect within this particular domain. In some situations, users can choose between different authentication schemes [31], and the decoy effect might help to guide users more effectively.

<sup>4</sup><https://pgs.ece.cmu.edu/> last access on May 10th 2016



## REFERENCES

- [1] D. Kahneman and A. Tversky, "Choices, Values, and Frames," *American Psychologist*, vol. 39, no. 4, pp. 341–350, 1984.
- [2] J. Huber, J. W. Payne, and C. Puto, "Adding Asymmetrically Dominated Alternatives: Violations of Regularity and the Similarity Hypothesis," *Journal of Consumer Research*, vol. 9, no. 1, p. 90, 1982.
- [3] D. Weirich and M. A. Sasse, "Pretty Good Persuasion: A First Step towards Effective Password Security in the Real World," in *Proceedings of the 2001 Workshop on New Security Paradigms (NSPW '01)*. New York, NY, USA: ACM, 2001, pp. 137–143. [Online]. Available: <http://dl.acm.org/citation.cfm?id=508195>
- [4] S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley, "Does My Password Go Up to Eleven?: The Impact of Password Meters on Password Selection," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*, 2013, pp. 2379–2388. [Online]. Available: <http://doi.acm.org/10.1145/2470654.2481329>
- [5] M. D. Leonhard and V. N. Venkatakrishnan, "A Comparative Study of Three Random Password Generators," in *2007 IEEE International Conference on Electro/Information Technology, EIT 2007*. IEEE, 2007, pp. 227–232.
- [6] D. Lockton, "Cognitive Biases, Heuristics and Decision-Making in Design for Behaviour Change," 2012. [Online]. Available: [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2124557](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2124557)
- [7] D. Ariely and T. S. Wallsten, "Seeking Subjective Dominance in Multidimensional Space: An Explanation of the Asymmetric Dominance Effect," *Organizational Behavior and Human Decision Processes*, vol. 63, no. 3, pp. 223–232, 1995. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0749597885710758>
- [8] R. H. Thaler and C. R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness*. Yale University Press, 2008. [Online]. Available: <https://books.google.com/books?hl=de&lr=&id=dSJQn8egXvUC&pgis=1>
- [9] R. H. Thaler, C. R. Sunstein, and J. P. Balz, "Choice architecture," *Social Science Research Network*, no. August, 2010. [Online]. Available: <http://ssrn.com/abstract=1583509>
- [10] L. Coventry, P. Briggs, D. Jeske, and A. V. Moorsel, "SCENE : A Structured Means for Creating and Evaluating Behavioral Nudges in a Cyber Security Environment," in *Design, User Experience, and Usability. Theories, Methods, and Tools for Designing the User Experience*, 8517th ed., A. Marcus, Ed. Springer International Publishing, 2014, pp. 229–239.
- [11] S. Egelman, A. P. Felt, and D. Wagner, "Choice Architecture and Smartphone Privacy: Theres A Price for That," in *The economics of information security and privacy*, R. Böhme, Ed. Springer, 2013, pp. 211–236.
- [12] A. Jameson, S. Gabrielli, P. O. Kristensson, K. Reinecke, F. Cena, C. Gena, and F. Vernerio, "How can we support users' preferential choice?" *Proceedings of the 2011 annual conference extended abstracts on Human factors in computing systems - CHI EA '11*, p. 409, 2011. [Online]. Available: <http://portal.acm.org/citation.cfm?doid=1979742.1979620>
- [13] S. Korff and R. Böhme, "Too Much Choice: End-User Privacy Decisions in the Context of Choice Proliferation," in *Symposium on Usable Privacy and Security (SOUPS '14)*, 2014, pp. 69–87. [Online]. Available: <https://www.usenix.org/system/files/soups14-paper-korff.pdf>
- [14] R. Shay, P. G. Kelley, S. Komanduri, M. L. Mazurek, B. Ur, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor, "Correct Horse Battery Staple," in *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. New York, NY, USA: ACM, 2012, pp. 1–20. [Online]. Available: <http://dl.acm.org/citation.cfm?doid=2335356.2335366>
- [15] R. Shay, S. Komanduri, A. L. Durity, P. S. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, and L. F. Cranor, "Can Long Passwords Be Secure and Usable?" in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*, 2014.
- [16] M. Keith, B. Shao, and P. Steinbart, "A Behavioral Analysis of Passphrase Design and Effectiveness," *Journal of the Association for Information Systems*, vol. 10, no. 2, pp. 63–89, 2009. [Online]. Available: <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1492&context=jais>
- [17] B. Ur, P. G. Kelley, S. Komanduri, J. Lee, M. Maass, M. L. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor, "How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation Bias," in *Security '12 Proceedings of the 21st USENIX conference on Security symposium*, 2012, pp. 5–16. [Online]. Available: <https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final209.pdf>
- [18] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman, "Of Passwords and People," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*, 2011, pp. 2595–2604. [Online]. Available: <http://dl.acm.org/citation.cfm?doid=1978942.1979321>
- [19] B. J. Fogg, *Persuasive Technology: Using Computers to Change What We Think and Do*. San Francisco, CA, USA: Morgan Kaufmann, 2003.
- [20] A. Forget, S. Chiasson, P. C. Van Oorschot, and R. Biddle, "Improving Text Passwords Through Persuasion," in *Proceedings of the 4th Symposium on Usable Privacy and Security (SOUPS '08)*. New York, NY, USA: ACM, 2008, pp. 1–12. [Online]. Available: <http://portal.acm.org/citation.cfm?id=1408666>
- [21] A. Forget and R. Biddle, "Memorability of Persuasive Passwords," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '08)*, 2008, p. 3759. [Online]. Available: <http://portal.acm.org/citation.cfm?doid=1358628.1358926>
- [22] T. Seitz, "The Decoy Effect for Passwords - A First Exploration," Ludwig-Maximilians-Universität München, Munich, Tech. Rep., 2016.
- [23] S. S. Iyengar and M. R. Lepper, "When Choice is Demotivating: Can One Desire Too Much of a Good thing?" *Journal of Personality and Social Psychology*, vol. 79, no. 6, pp. 995–1006, 2000.
- [24] R. M. Ryan and E. L. Deci, "Self-Determination Theory and the Facilitation of Intrinsic Motivation," *American Psychologist*, vol. 55, no. 1, pp. 68–78, 2000.
- [25] P. Inglesant and M. A. Sasse, "The True Cost of Unusable Password Policies: Password Use in the Wild," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*, 2010, pp. 383–392. [Online]. Available: <http://eprints.ucl.ac.uk/102754/>
- [26] M. L. Mazurek, S. Komanduri, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, P. G. Kelley, R. Shay, and B. Ur, "Measuring password guessability for an entire university," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security - CCS '13*, 2013, pp. 173–186. [Online]. Available: <http://dl.acm.org/citation.cfm?doid=2508859.2516726>
- [27] E. Von Zezschwitz, A. De Luca, and H. Hussmann, "Honey , I Shrank the Keys : Influences of Mobile Devices on Password Composition and Authentication Performance," in *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational (NordCHI '14)*. New York, NY, USA: ACM, 2014, pp. 461–470.
- [28] D. L. Wheeler, "zxcvbn: Low-budget password strength estimation," in *25th USENIX Security Symposium (USENIX Security 16)*. Austin, TX: USENIX Association, Aug. 2016, to appear. Author provided pre-print.
- [29] B. Ur, S. M. Segreti, L. Bauer, N. Christin, L. F. Cranor, S. Komanduri, D. Kurilova, M. L. Mazurek, W. Melicher, and R. Shay, "Measuring Real-World Accuracies and Biases in Modeling Password Guessability," in *24th USENIX Security Symposium (USENIX Security 15)*. USENIX Association, 2015, pp. 463–481. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/ur>
- [30] D. Ashenden and D. Lawrence, "Can We Sell Security Like Soap? A New Approach to Behaviour Change," in *New Security Paradigms Workshop (NSPW '13)*, 2013, pp. 87–94. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2535823>
- [31] A. Forget, S. Chiasson, and R. Biddle, "Choose Your Own Authentication," in *Proceedings of the New Security Paradigms Workshop (NSPW '15)*. Twente, The Netherlands: ACM, 2015.



APPENDIX

TABLE I

SUMMARIES OF PASSWORD METRICS FROM THE ONLINE EXPERIMENT.  
ARRANGED BY GROUP (COLUMNS) AND METRIC (ROWS)

	Control		Mangled		Words		Decoy	
	M	SD	M	SD	M	SD	M	SD
length	11.33	3.53	11.8	2.74	13.87	3.8	11.9	2.69
score	2.88	1.02	2.9	0.76	3.29	0.9	2.95	0.88
guesses <sub>log10</sub>	8.84	2.41	8.86	2.15	13.48	7.63	10.12	4.85
digits	2.61	2.06	2.28	1.27	2.16	2.18	2.6	2.34
special	0.22	0.64	0.52	1.16	0.2	0.5	0.3	0.57
uppercase	1.77	0.8	1.42	0.59	2.45	2.35	1.75	1.11
lowercase	6.55	3.91	7.38	3.21	8.91	4.09	6.95	3.42

TABLE II

POLICY FULFILLMENT OF SUBMITTED PASSWORDS. MOST PARTICIPANTS  
USED AT LEAST THREE CHARACTER CLASSES.

	comp8	3class8	3class12	3class16	basic8	basic12	basic16
Control	2	9	4	0	1	1	1
Mangled	6	7	3	3	1	1	0
Words	4	5	4	2	1	1	7
Decoy	5	7	3	1	1	1	2
$\Sigma$	17	28	14	6	4	4	10

# On the impact of warning interfaces for enabling the detection of Potentially Unwanted Applications

Vlasta Stavova & Vashek Matyas  
Faculty of Informatics  
Masaryk University, Czech Republic  
Email: vlasta.stavova@mail.muni.cz, matyas@fi.muni.cz

Mike Just  
School of Mathematical & Computer Sciences  
Heriot-Watt University, United Kingdom  
Email: m.just@hw.ac.uk

**Abstract**—We conducted a large-scale online study with 26,000 software installations during which we asked user (participants) whether they wanted to enable or disable the detection of Potentially Unwanted Applications (PUAs – potentially malicious software, such as *adware* or *spyware*). PUAs are notoriously difficult to manage, e.g., legal challenges can preclude default options that could otherwise be set for PUAs detection or removal. Our study was performed with an IT security software provider (ESET) who gave us access to the participants (antivirus product beta users). We used a between-subjects design with 15 conditions (a starting-point control interface, and 14 new “warning” interfaces). Despite the fact that many software companies (e.g., Microsoft, AVAST, AVG, McAfee, Kaspersky Lab) are struggling with PUAs detection, there are few studies focused on this topic.

Our results indicate a strong desire for PUAs detection by users. In particular, enabling PUAs detection was chosen by 74.5% of our participants for our initial control interface. Further, a modified interface in which the option to enable PUAs detection was *presented first* resulted in 89.8% of participants choosing to enable PUAs detection (a *statistically significant increase from the control*).

## I. INTRODUCTION

A *potentially unwanted application (PUA)* is software, such as *adware* or *spyware*, that can collect information about users [1]. PUAs are traditionally installed locally on a user’s machine, though they can also operate via web-based mechanisms, for example using cross-site scripting [2]. Like malware, PUAs use computing resources, such as memory, processes and networks, and can also have a negative impact on user privacy, e.g., by collecting information such as page interactions and search queries. While malware is often deemed more malicious (e.g., supporting fraud, theft, denial-of-service), the direct results of PUAs are typically perceived as more benign and (legally or ethically) ambiguous. For this reason, PUAs are sometimes referred to as *greyware* [3]. While malware is typically subjected to automatic removal,

the removal of *PUAs* will often depend upon the choice of a user [4].

While there has been a significant focus on malware over the years (e.g., [5], [6], [7]), there has been less focus on PUAs. Furnell et al. [8] highlight the impact that this has in terms of properly quantifying cybercrime, for example. However, recent research has provided an excellent first step, with a comprehensive analysis of the means and scale of adware injection [2]. Yet despite the fact that many software companies (such as Microsoft [9], AVAST [10], AVG [11], McAfee [12] and Kaspersky Lab [13]) are dealing with PUAs detection warnings, there appears to be no other study focused on this topic. In our paper, recognizing the importance of user involvement in deciding whether to accept a PUAs detection or not, we focus on the impact of warning interfaces for encouraging users to enable the detection of PUAs.

Deciding whether to enable PUAs detection is conceptually similar to other activities, such as controlling malware installation [14], evaluating whether mobile applications respect privacy [15], updating software [16] and click-through agreements [17], as each encourages a user to make an informed decision. Though due to the dubious legal standing of PUAs and their arguably lower risk (compared to malware) [18], it can be challenging to describe the threat of PUAs to users. For example, since the developers of PUAs actively defend their products, PUAs installation warnings that are overly biased (against their installation) can provoke legal challenges [3].

In this paper we report on a large-scale online study with 26,000 software installations in which we evaluated the effectiveness of a set of “unbiased warning” (i.e., warnings without intentionally stressed options) interfaces that asked participants (who were in the process of installing their antivirus software) whether they wanted to enable a feature that would thereafter detect the installation of PUAs.<sup>1</sup> Our designs were “unbiased” in the sense that we tried to present information and choices using non-judgemental language with regard to the acceptability of PUAs. Our goal was to *increase the number of participants who enabled PUA detection* when compared to the starting-point control interface. We were somewhat limited in the scale of interface changes that we could make (note that

Permission to freely reproduce all or part of this paper for noncommercial purposes is granted provided that copies bear this notice and the full citation on the first page. Reproduction for commercial purposes is strictly prohibited without the prior written consent of the Internet Society, the first-named author (for reproduction of an entire paper only), and the author’s employer if the paper was prepared within the scope of employment.  
EuroUSEC ’16, 18 July 2016, Darmstadt, Germany  
Copyright 2016 Internet Society, ISBN 1-891562-45-2  
<http://dx.doi.org/10.14722/eurousec.2016.23003>

<sup>1</sup>Full paper details and author contact information will be found at <http://crs.cs/papers/eurousec2016>.

these changes were made to the live system of our industry partner) so that more comprehensive changes were not possible for this experiment. Our interface designs and the evaluation study were performed in cooperation with the IT security software provider ESET who provided access to the study participants (antivirus product beta testers). Our 15 interface variations were based on four categories of warning features, namely (i) use of simple, jargon-free descriptions, (ii) warning images, (iii) enhanced text, such as with colour or bolding, and (iv) altering the order of option choices. Our reported results are quantitative and consist of the number of participants that decided to enable the PUAs detection feature (or not) for each of the interface variations.

In Section II we describe the related work in the area of warning design. Section III introduces principles and variables used during the design of proposed variants and also specifies the experiment design. Section IV explains the most significant experiment findings, while Section V discusses further observations. We conclude in Section VI. The appendix contains all proposed variants of PUAs detection user dialogs.

## II. RELATED WORK

Previous work on security warnings tends to focus on either the *content* of the warning or the *presentation* of the warning. The end goal is to increase either adherence to a warning, or comprehension of the warning or its potential impacts. In some cases, where there are repeated requests for a user to respond to a warning, factors such as habituation are considered. While habituation does become an issue when managing each individual PUA, in this paper we focus primarily on the decision to enable (or not) a PUAs detection feature during one-time installation. Habitual choices related to each PUA acceptance decision will be considered in our future studies. In terms of warning message, there are conflicting results regarding the effectiveness of detailed explanations. Bravo-Lillo et al. [19] showed that a detailed explanation did not work well as an attractor in an experiment with other attractors (such as the use of pictorial symbols, colours, framing, etc.). Whereas Tan et al. [20] found that warning with a “purpose string” has a higher (but still not statistically significant) impact on a user over a warning without any purpose. Providing an example makes users pay more attention and consequently make more risk-aware choices [21].

Text structure may enhance readability too. Warning text in bullets or in an outline form is considered more readable than continuous text [22]. Use of simple language is also recommended. In terms of warning presentation, graphical improvements are often used to catch users’ attention. For example, users are more likely to read salient, eye-catching warnings [23].

Wogalter et al. [24] note that warning visibility and readability can be enhanced by large or bold print that contrasts with the standard type and by adding signal colours, borders and special effects like flashing lights. User’s comprehension can be increased also by adding pictorials to the warning [25]. Signal safety words, for example “Warning”, “Danger”,

“Caution” or “Notice” also increase users’ perceptions of a potentially risky situation [26].

Aspects such as colour, option order and pictorials have recently been used to *slightly influence*, or “nudge” users to use more secure options. For example, Turland et al. [27] designed a prototype for nudging users to select more secure wireless access points. Option order (the secure option comes first), option colour and the effect of pictorials were tested. There was a significant increase in choosing safer options depending on the colour of options, and their order, though a padlock pictorial had a negative impact (it tended to puzzle users).

Felt et al. [28] recently redesigned Google Chrome’s SSL warning and tested the proposals with microsurveys and a field study. They used simple language, avoided technical jargon, targeted wording to a low reading level, and provided a short description. Despite using such (previously recommended) design features, they failed in designing a comprehensible warning, though they did increase adherence. The use of pictorial symbols and contrasting colours (yellow and gray) were main parts of the new design. In particular, the variant with a gray background and simple, jargon-free text had the best performance.

Other techniques such as *persuasion* [29] have also been used in computer security, such as for improving password choices, and anti-virus behaviour [30], [31]. There is also design example in which users are encouraged to update their first password choice by adding new characters [30].

## III. INTERFACE DESIGN AND EVALUATION

### A. Interface Design

For our studies, we used a baseline interface (see Fig. 1) that contained a short paragraph with a brief explanation of PUAs detection importance. “*ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer’s performance, speed and reliability, or cause changes in behavior. They usually require user’s consent before installation.*” People show their agreement by picking an option “Disable detection of potentially unwanted applications.” or by choosing other option “Enable detection of potentially unwanted applications.” To avoid potential legal challenges related to setting a default “enable detection” option, our interface designs used unchecked ‘radio buttons’ so that participants were required to choose one of the two options. There is one more user dialog that appears on the same screen that asks users to join “LiveGrid”<sup>2</sup>. Drawing on previous work on security warnings we tested 14 variations from the control interface that alter features such as the warning description (e.g., with hyperlinks, bullets) or presentation (e.g., with images, bolding, simple language, option order). We observed whether the application of these techniques to enabling PUAs detection had positive or negative

<sup>2</sup>ESET LiveGrid collects data submitted by ESET users worldwide and sends it to their malware research labs for analysis [32].

effects on user adherence, when compared to their use for other warning purposes.

Changes we made may seem subtle, but a conceptual redesign was out of question due to several limitations imposed by the company. However, we feel that even with our “subtle” changes we were able to incorporate some traditional warning design features.

Newly designed variants (marked A-N) are described in Appendix and are summarized in Table I along with their corresponding variant label. The interfaces of Variants A to K are shown in Figures 2 and 3 in the Appendix as they would have been viewed by our study participants (the LiveGrid portion of the screen is not shown in these images due to space constraints). Although the LiveGrid is strictly separate to our experiment, we wanted to investigate its impact on our participants, hence Variants L and N do not include LiveGrid user dialog on the same screen as the PUAs detection user dialog.

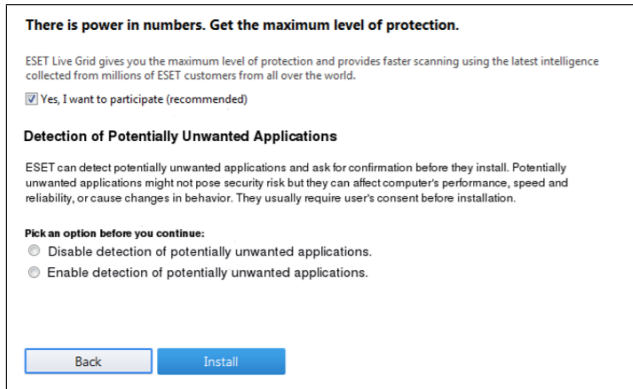


Fig. 1. The starting-point control variant.

1) *Option order and language:* In order to investigate the impact of changing options from the starting-point variant, we used three variants. In the first one, the order of the options was simply reversed (A in Fig. 2) so that “Enable detection of PUAs.” came first and “Disable detection of PUAs.” was second. In the second variant, we changed the wording so that “Disable detection of PUAs.” became “Don’t detect PUAs.” and “Enable detection of PUAs.” became simply “Detect PUAs” (B in Fig. 2). Since the formulation “Detect PUAs” is shorter and more straightforward than “Enable detection of PUAs”, we had anticipated (based on previous research [28]) that variant B would increase the success rate. For the third variant, we reversed the order with the new wording to give the option of “Detect PUAs.” first, and then “Don’t detect PUAs.” (C in Fig. 2). It is a combination of variants A and B.

2) *Hyperlink:* The role of explanation in warning design is still unclear. We wanted to investigate this issue so we designed three variants (D, E, F in Fig. 2) with a hyperlink connecting to the company website where a detailed PUAs explanation is provided. Variants D (Fig. 2) and E (Fig. 2) differ only in a text formulation of the hyperlink. Variant D (Fig. 2) states “What is a potentially unwanted application?”,

whereas variant E (Fig. 2) is “Why do we ask?” Variant F (Fig. 2) contains the hyperlink with the text “What is a potentially unwanted application?” but without the whole explanatory paragraph. The main aim of this variant was to investigate whether participants are influenced by moving the explanation from the warning body to an external web page or not.

3) *Pictorials:* Since related work considers pictures, pictorials or alert signs to be powerful attractors, we wanted to test this assumption also for the PUAs detection issue. We designed two variants (G, H in Fig. 3) where pictorials are added to the warning. Variant G (Fig. 3) uses the standard company warning sign, whereas variant H (Fig. 3) has the ANSI warning triangle.

4) *Providing an example:* People are more likely to adhere to a warning when they see a purpose. To provide a purpose to this warning, we decided to design a variant (I in Fig. 3) where an example is added at the end of the paragraph text. The sentence is: “**For example**, they may change your web browser’s web page and search settings.”

5) *Signal word and signal red colour:* As well as pictorial symbols, signal words and bright colours are also considered to be good attractors. To test this assumption, we designed the variant (J in Fig. 3) in which the paragraph text is introduced by the signal word “Notice” in red-coloured text. We expected that the combination of the colour and the signal word would catch users’ attention and stress the importance of the user dialog.

6) *Bulleted text:* Since structured text is considered to be more readable than text in a single block, we designed variant K (Fig. 3), in which the text block is separated into bullet list. Also, the important words in the paragraph text – “**can affect your computer’s:**” are presented in a bold type.

7) *Complex combinations:* Finally, we also included some more complex variants that combined or removed features of at least three existing variants. For these variants, we do not provide the corresponding images. In variant L, we investigated the influence of separating the PUAs detection and LiveGrid user dialog. We assumed that separating PUAs detection user dialog would enhance its visibility to participants. During the process of design, we identified a couple of variables that we wanted to test together to amplify their strength. The first combined variant, M, consists of a combination of text structure (K in Fig. 3), reformulated text in options (B in Fig. 2) and an explanatory hyperlink (D in Fig. 2). The other combined variant N has a similar structure to M, the only additional change being the removal of the previous (LiveGrid) user dialog.

8) *Persuasion (not applied):* For our purposes, persuasive techniques were viewed as too biased. For example, consider designs in which users are encouraged to update their first password choice by adding new characters [30] – we felt that it would be too much of a bias if a user were asked to reconsider their first choice of choosing to disable PUAs detection. Similarly, we considered an option whereby a user might be encouraged to follow the decision of others (e.g., by suggesting that “80% of other customers chose to enable PUAs

Var.	Description
Control	Text description with “Disable detection”, then “Enable detection”(see Fig. 1).
A	<i>Option order reversed</i> : “Enable detection”, then “Disable detection”.
B	<i>Option text changed</i> : from “Don’t detect” to “Detect”.
C	<i>Option text changed &amp; reversed</i> : Combines A and B.
D	<i>Added hyperlink</i> : “What is a potentially unwanted application?”
E	<i>Added hyperlink</i> : “Why do we ask?”
F	<i>Added hyperlink &amp; no text description</i> : “What is a PUA?”
G	<i>Added warning image</i> : Warning image provided by the company.
H	<i>Added warning image</i> : ANSI warning triangle.
I	<i>Added example</i> : Added a practical example to end of description.
J	<i>Coloured warning text</i> : Added red <i>Notice</i> to start of text description.
K	<i>Bulleted text</i> : Text description bulleted, with partial bolding.
L	<i>LiveGrid user dialog</i> : LiveGrid user dialog removed from the screen.
M	<i>Hyperlink, bulleted text, &amp; option text changed</i> : Combines B, D, K.
N	<i>Combination B, D, K, L</i> .

TABLE I  
SUMMARY DESCRIPTION OF TESTED VARIANTS. SEE FIGS 2 AND 3 FOR SCREEN IMAGES OF VARIANTS A TO K.

detection”), though this too was felt to be overly biased (even though statistics would legitimately reflect previous customer behaviour).

### B. Experiment

The experiment ran in June and July 2015. We cooperated with ESET and used their proprietary system to measure a success rate of each variant. Since PUAs can have harmful effects, we defined our *success rate* as the percentage of antivirus installations where participants enabled PUAs detection during antivirus installation. We treated each variant as a condition in between-subjects experiment, including our 14 new design variants and the control one. Participants were product beta users who installed a beta version of ESET antivirus software. We had more than 26,000 SW installations in total, i.e. 1,755 per variant on average. Other more precise measurements, for example one case per device, were not possible in our study since we used the existing data collection interfaces of our industrial partner.

Each case in our dataset represented one antivirus installation. Unfortunately, we can not detect a situation when one same participant installed antivirus on multiple different devices.

Concerning that we are examining a beta version of a home end-point antivirus solution, we do not expect that many people will behave this way. For example, administrators usually do not install antivirus beta version across the entire site they administer. It is also hard to detect situations where somebody would have installed multiple times the beta version of the ESET antivirus solution on the same device. Since we collect for each installation the device IP address, CPU, RAM and OS platform, we found out that cases with same values in this attributes make only a small percentage of the whole dataset.

Each participant was randomly assigned to a variant. See Table II for a summary of our results of performing pairwise comparisons of each variant to the starting-point control interface.

Var.	No. of installations	Succ. rate	p-value	Sign.
Control	1,759	74.5%		
A	1,796	89.8%	0.001	YES
B	1,734	72%	0.1	no
C	1,755	83.9%	0.001	YES
D	1,766	72.8%	0.25	no
E	1,749	72.6%	0.21	no
F	1,688	72.7%	0.23	no
G	1,730	73.7%	0.6	no
H	1,735	73.1%	0.35	no
I	1,818	73.3%	0.41	no
J	1,772	71.1%	0.037	no
K	1,809	71.6%	0.052	no
L	1,699	73%	0.82	no
M	1,780	72.8%	0.25	no
N	1,737	73.6%	0.57	no

TABLE II  
SUMMARY OF RESULTS FOR ALL VARIANTS. FINAL COLUMN INDICATES WHETHER THE SUCCESS RATE WAS SIGNIFICANTLY DIFFERENT (STATISTICALLY) FROM THE CONTROL VARIANT.

## IV. FINDINGS

The control variant had a success rate 74.5%. The average success rate of all tested variants in total is 74.7%. The highest success rate, 89.8%, was achieved with the variant A (Fig. 2) where the order was changed (in comparison with the starting-point variant) – the first option is “Enable detection of PUAs.” and the second is “Disable detection of PUAs.” The lowest success rate was for variant J (see Fig. 3). To correct for the alpha error inflation resulting from multiple  $\chi^2$  testing, we used the significance level  $\alpha=0.05/16=0.003$  to find statistically significant differences among variants.

### A. Option order and language

Observing the ordering and language for the “Enable detection of PUAs/Disable detection of PUAs” options, we evaluated and compared variants A, B and C (see Fig. 2) with the control variant (see Fig. 1). The control variant had a success rate 74.5%, while the rate changed to 89.8% for variant A with order changed, 72% for variant B where a shorter, reformulated text was used with the same order of the

control variant, and 83.9% for variant C which combined both language and order changes from the control variant.

1) *Option order*: We used  $\chi^2$  test at the significance level  $\alpha=0.003$  to find statistically significant differences among variants that differ only in the order of options. The order of options really matters for PUAs detection, as with other types of warnings, e.g., [27]. We showed that users have a strong tendency to choose the first option, irrespective of whether it is for a positive or negative installation choice. We used the  $\chi^2$  test to compare the control variant with variant A (Fig. 2) where “Enable detection of PUAs” came first and “Disable detection of PUAs” ( $\chi^2=143$ ,  $p<0.001$ ,  $df=1$ ,  $r=0.2$ ,  $OR=3.02$ ) came second. A statistically significant increase in the success rate towards the variant with switched order was observed. Then we used the  $\chi^2$  test to compare the control variant with variant C (Fig. 2) ( $\chi^2=48$ ,  $p<0.001$ ,  $df=1$ ,  $r=0.116$ ,  $OR=1.79$ ), and the result was very similar. Our subjects were more likely to pick the first option they were offered.

When we merged the results from the two variants, where the first option is positive (variants A and C) into one, and by a similar process we made with two variants, where the first option was formulated negatively (B and control), we used the  $\chi^2$  test and we found out that the position on the first place is a very strong aspect to influence the user to pick the preferred option ( $\chi^2=206$ ,  $p<0.001$ ,  $df=1$ ,  $r=0.171$ ,  $OR=0.412$ ).

2) *Option language*: Considering the option text language, the formulation “Enable detection of PUAs” (A in Fig. 2) has a higher influence ( $\chi^2=27$ ,  $p<0.001$ ,  $df=1$ ,  $r=0.087$ ,  $OR=0.592$ ) on users than “Detect PUAs” (C in Fig. 2), though both offer the option for enabling detection first. This difference is statistically significant.

In contrast, the control variant compared with variant B is not statistically significant ( $\chi^2=2.66$ ,  $p=0.1$ ,  $df=1$ ,  $r=0.027$ ,  $OR=0.882$ ).

### B. Warning image

According to previous research, a warning picture would catch the user’s attention and would increase the success rate more than the control variant [25]. We compared the variant without the pictorial symbols (the control one) and with the pictorial (G in Fig. 3) – the company’s warning sign ( $\chi^2=0.27$ ,  $p=0.6$ ,  $df=1$ ,  $r=0.009$ ,  $OR=0.96$ ), we observed that there is no significant difference in user behaviour. Similarly, when doing a comparison between the control variant and variant H (Fig. 3) with the ANSI warning triangle ( $\chi^2=0.87$ ,  $p=0.35$ ,  $df=1$ ,  $r=0.016$ ,  $OR=0.93$ ), no statistically significant difference is observed.

Finally, we compared both variants with the pictorial symbol ( $\chi^2=0.17$ ,  $p=0.68$ ,  $df=1$ ,  $r=0.007$ ,  $OR=0.969$ ). There is no significant difference in use of the standardized ANSI pictorial or the company’s own warning sign.

### C. Coloured warning text

We chose the red signal colour in combination with the warning word “Notice”. Both the use of a red colour and warning text has previously shown to be a good attractor [24].

Thus, we had expected that this attractor would increase the success rate. However, when comparing the “Notice” variant (J in Fig. 3) with the control variant ( $\chi^2=5.06$ ,  $p=0.024$ ,  $df=1$ ,  $r=0.037$ ,  $OR=0.843$ ), we found that the variant with “Notice” had no significant effect on the success rate from the control variant. This variant has the lowest success rate 71.1% from all variants (the control has 74.5%). One possible explanation for this result may be that some users misinterpreted the red colour as a warning to not add the PUAs detection feature, and thus clicked on the first option (“Disable detection of potentially unwanted applications”). This possibility also supports previous work on SSL warnings. Bravo-Lillo et al. improved SSL warnings adherence by stressing important parts by adding contrast color [19]. Despite the fact that this variant did not have best performance, still was better than the control one. Felt et al. [28] used signal color in warning design and significantly improved adherence of SSL warning. But both used “safe option” as the first option, whereas the safe option in our case was the second.

## V. OTHER FINDINGS

### A. Hyperlink

1) *Text in a hyperlink*: We were curious whether participants would be interested in more information and would be more likely to enable the PUAs detection in the variant that contains a hyperlink to the explanatory webpage. We also tested two variants of a descriptive hyperlink text. Current research considers explanation to be a bad attractor; on the other hand, users are more likely to behave securely if they see a purpose to this behaviour. We tested two possible formulations of this link. The company’s question mark pictorial symbol is appended to both sentences. The first is “Why do we ask?” (E in Fig. 2) and the second is “What is a potentially unwanted application?” (D in Fig. 2). We observed that there is absolutely no difference in user behaviour when formulations differ. ( $\chi^2=0.01$ ,  $p=0.92$ ,  $df=1$ ,  $r=0.001$ ,  $OR=1.00$ ). Unfortunately, our industry partner couldn’t provide us information whether users clicked on the hyperlink.

2) *Hyperlink and no description*: We expected that the version with the explanatory paragraph text (the control one) would increase the success rate more than the version without the explanatory paragraph text, but with a hyperlink only (F). The  $\chi^2$  test proved that there is no statistically significant difference between the variant with the explanatory paragraph text (the control variant) and the variant without explanatory text, only with the hyperlink following to the company’s web page with detailed explanation ( $\chi^2=1.41$ ,  $p=0.23$ ,  $df=1$ ,  $r=0.02$ ,  $OR=0.912$ ).

### B. Providing an example

We expected that the variant with the PUA example explicitly mentioned (I) in the text would increase the success rate over the control variant, because participants would see the purpose of PUAs detection clearly. Despite our expectations, providing the example in a bold type did not significantly

improve the success rate ( $\chi^2=0.67$ ,  $p=0.41$ ,  $df=1$ ,  $r=0.013$ ,  $OR=0.939$ ).

### C. Text structure

We decided to structure the paragraph with the explanatory text into bullet points to enhance its readability and text comprehension. Since structured text is more readable by participants, we expected also an improvement in the success rate over the control variant. The very unexpected result was that the variant with the structured text (K in Fig. 3) has the second lowest success rate 71.6% and we observed no significant difference in comparison with the control variant with an unstructured text ( $\chi^2=3.7$ ,  $p=0.052$ ,  $df=1$ ,  $r=0.032$ ,  $OR=0.863$ ).

### D. Complex combinations

We expected that the variant without the previous LiveGrid user dialog (L in Fig. 3) would be more effective, as it would catch the user's attention better and increase the success rate. Comparing the control variant with the corresponding variant without the previous LiveGrid question ( $\chi^2=0.05$ ,  $p=0.82$ ,  $df=1$ ,  $r=0.003$ ,  $OR=0.928$ ), we observed no difference in user behaviour.

We expected that the variant with a combination of several principles would increase the user success rate more than variants with only one aspect used. Comparing the control variant with the "combined variant" (M in Fig. 3) that contained structured text, the hyperlink and a shorter text in options ( $\chi^2=1.355$ ,  $p=0.25$ ,  $df=1$ ,  $r=0.019$ ,  $OR=0.915$ ), no significant change in user behaviour was observed.

The combination of four aspects (N in Fig. 3) (a structured text, a hyperlink, a shorter option text and previous user dialog removal) also did not lead to significant improvements ( $\chi^2=0.32$ ,  $p=0.57$ ,  $df=1$ ,  $r=0.009$ ,  $OR=0.957$ ) in comparison with the control variant.

## VI. CONCLUSIONS

We conducted our user experiment in the unexplored area of the acceptability of potentially unwanted applications (PUAs). PUAs are notoriously difficult to manage, e.g., legal challenges can preclude default options that could otherwise be set for PUAs detection or removal. Our large-scale experiment was completed with 26,000 SW installations. It was conducted in cooperation with antivirus product beta version users of the IT security software provider ESET. Drawing on previous security warning literature, we tested the impact of 15 warning screen variations for their ability to encourage participants to enable PUAs detection during the process of antivirus installation.

Starting with the control variant, we determined that 74.5% of participants wanted to enable PUAs detection. Further, from our 15 variants, we obtained an even larger percentage by presenting a positive option first (for enabling the PUAs detection), resulting in a statistically significant increase to 89.8% adherence (an increase of 15.3 percentage points). This best variant also has the highest effect size (odds ratio)

3.02. Further research will be needed to evaluate user trust level towards security products and his behaviour during its installation.

The remaining variants, covering effects such as warning images, bolding, red-coloured "Notice" and simplified warning text were surprising for not providing any increase in the number of participants who enabled PUAs detection. Odds ratios in this cases were around 0.9. In fact, the use of a signal word *Notice* in a contrasting red colour resulted in the lowest success rate 71.1%. While the results about the order of options may not seem that surprising, the variability of success between all options, some of which we would have also expected an increase, e.g., option J (coloured warning text) is very surprising, especially given the previous positive effects of these warning techniques, e.g., for SSL warning adherence.

The main conclusion from our results is that the order of available options is crucial. The design change with the greatest impact in a limited design space is to simply put the "safe option" in the first place.

Our study focuses only on the behavior of beta users. It could be enhanced by collecting statistics about clicking on hyperlinks in variants D, E and F and also by more precise distinction between multiple installations under single user credentials in our dataset. This was not possible in the current study as we used the existing data collection interfaces of our industry partner.

In future work, there are a number of areas for potential improvement and further advancement. We plan to perform a similar evaluation on a more diverse set of participants (e.g., not only beta users, but also real product users), and also to collect further data, including qualitative feedback from participants. We also plan to investigate more on antivirus users demography and security and privacy attitudes.

## ACKNOWLEDGMENT

The authors acknowledge the support of the Masaryk University (MUNI/M/1052/2013). Thanks also to the reviewers for their excellent feedback, and to our shepherd (Paul Gerber) for his assistance in greatly improving the presentation of our results.

## REFERENCES

- [1] J. C. Sipior, B. T. Ward, and G. R. Roselli, "The ethical and legal concerns of spyware," *Information Systems Management*, vol. 22, no. 2, pp. 39–49, 2005.
- [2] K. Thomas, E. Bursztein, C. Grier, G. Ho, N. Jagpal, A. Kapravelos, D. McCoy, A. Nappa, V. Paxson, P. Pearce, N. Provos, and M. Abu Rajab, "Ad injection at scale: Assessing deceptive advertisement modifications," in *Security and Privacy (SP), 2015 IEEE Symposium on*, May 2015, pp. 151–167.
- [3] J. Malcho, "Is there a lawyer in the lab?" in *Proceedings of the 19th Virus Bulletin International Conference*, 2009.
- [4] A. Butcher, J. Garms, K. Azad, M. Seinfeld, P. Bryan, S. Reasor, and A. Loh, "Identifying and removing potentially unwanted software," Mar. 23 2010, uS Patent 7,685,149. [Online]. Available: <https://www.google.com/patents/US7685149>
- [5] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*. ACM, 2011, pp. 3–14.



- [6] E. Gandotra, D. Bansal, and S. Sofat, "Malware analysis and classification: A survey," *Journal of Information Security*, vol. 2014, 2014.
- [7] M. Wagner, F. Fischer, R. Luh, A. Haberson, A. Rind, D. A. Keim, W. Aigner, R. Borgo, F. Ganovelli, and I. Viola, "A survey of visualization systems for malware analysis," in *Eurographics Conference on Visualization (EuroVis) State of The Art Reports*. EuroGraphics, 2015, pp. 105–125.
- [8] S. Furnell, D. Emm, and M. Papadaki, "The challenge of measuring cyber-dependent crimes," *Computer Fraud & Security*, vol. 2015, no. 10, pp. 5–12, 2015.
- [9] "How Microsoft antimalware products identify malware: unwanted software and malicious software," <https://www.microsoft.com/security/portal/mmpc/shared/objectivecriteria.aspx>, accessed: 2016-06-17.
- [10] "Avast: Enable detection of potentially unwanted programs (PUPs)," <http://ccm.net/faq/15731-avast-enable-detection-of-potentially-unwanted-programs>, accessed: 2016-06-17.
- [11] "What are Potentially Unwanted Programs (PUP)," [https://support.avg.com/SupportArticleView?l=en\\_US&urlName=What-is-Potentially-Unwanted-Program-PUP](https://support.avg.com/SupportArticleView?l=en_US&urlName=What-is-Potentially-Unwanted-Program-PUP), accessed: 2016-06-17.
- [12] "Potentially Unwanted Programs (PUPs)," <http://www.mcafee.com/us/threat-center/resources/pups-configuration.aspx#VSE7>, accessed: 2016-06-17.
- [13] "Kaspersky Internet Security 2011," <http://support.kaspersky.com/3914>, accessed: 2016-06-17.
- [14] D. Modic and R. Anderson, "Reading this may harm your computer: The psychology of malware warnings," *Computers in Human Behavior*, vol. 41, pp. 71–79, 2014.
- [15] O. Kulyk, P. Gerber, M. E. Hanafi, B. Reinheimer, K. Renaud, and M. Volkamer, "Encouraging privacy-aware smartphone app installation: Finding out what the technically-adept do," 2016. [Online]. Available: <http://eprints.gla.ac.uk/116161/>
- [16] K. E. Vaniea, E. Rader, and R. Wash, "Betrayed by updates: how negative experiences affect future security," in *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2014, pp. 2671–2674.
- [17] V. C. Plaut and R. P. Bartlett III, "Blind consent? a social psychological investigation of non-readership of click-through agreements," *Law and human behavior*, vol. 36, no. 4, p. 293, 2012.
- [18] "What is a potentially unwanted application or potentially unwanted content," <http://support.eset.com/kb2629/>, 2015, accessed: 2016-06-17.
- [19] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. Schechter, "Your Attention Please: Designing Security-decision UIs to Make Genuine Risks Harder to Ignore," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*, ser. SOUPS '13. New York, NY, USA: ACM, 2013, pp. 6:1–6:12. [Online]. Available: <http://doi.acm.org/10.1145/2501604.2501610>
- [20] J. Tan, K. Nguyen, M. Theodorides, H. Negrón-Arroyo, C. Thompson, S. Egelman, and D. Wagner, "The effect of developer-specified explanations for permission requests on smartphone user behavior," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '14. New York, NY, USA: ACM, 2014, pp. 91–100. [Online]. Available: <http://doi.acm.org/10.1145/2556288.2557400>
- [21] M. Harbach, M. Hettig, S. Weber, and M. Smith, "Using personal examples to improve risk communication for security & privacy decisions," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2014, pp. 2647–2656.
- [22] E. N. Wiebe, E. F. Shaver, and M. S. Wogalter, "People's beliefs about the internet: Surveying the positive and negative aspects," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 45, no. 15, pp. 1186–1190, 2001. [Online]. Available: <http://pro.sagepub.com/content/45/15/1186.abstract>
- [23] J. A. Strawbridge, "The influence of position, highlighting, and imbedding on warning effectiveness," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 30, no. 7. SAGE Publications, 1986, pp. 716–720.
- [24] M. S. Wogalter, V. C. Conzola, and T. L. Smith-Jackson, "Research-based guidelines for warning design and evaluation," *Applied ergonomics*, vol. 33, no. 3, pp. 219–230, May 2002.
- [25] J. S. Wolff and M. S. Wogalter, "Comprehension of pictorial symbols: Effects of context and test method," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 40, no. 2, pp. 173–186, 1998.
- [26] M. S. Wogalter, M. J. Kalsher, L. J. Frederick, and A. B. Magurno, "Hazard level perceptions of warning," *International Journal of Cognitive Ergonomics*, vol. 2, no. 1-2, pp. 123–143, 1998.
- [27] J. Turland, L. Coventry, D. Jeske, P. Briggs, and A. van Moorsel, "Nudging towards security: Developing an application for wireless network selection for android phones," in *Proceedings of the 2015 British HCI Conference*. ACM, 2015, pp. 193–201.
- [28] A. P. Felt, A. Ainslie, R. W. Reeder, S. Consolvo, S. Thyagaraja, A. Bettes, H. Harris, and J. Grimes, "Improving ssl warnings: Comprehension and adherence," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2015, pp. 2893–2902.
- [29] R. Cialdini, *Influence: The Psychology of Persuasion*. HarperCollins, 2009.
- [30] L. Zhang-Kennedy, S. Chiasson, and R. Biddle, "The role of instructional design in persuasion: A comics approach for improving cyber security," *International Journal of Human-Computer Interaction*, no. just-accepted, 2016.
- [31] A. Forget, S. Chiasson, P. C. van Oorschot, and R. Biddle, "Persuasion for stronger passwords: Motivation and pilot study," in *Persuasive Technology*. Springer, 2008, pp. 140–150.
- [32] "The ESET Advantage," <http://www.eset.com/us/about/eset-advantage/>, 2006, accessed: 2016-06-17.

APPENDIX  
PROPOSED PUAS DETECTION USER DIALOGS

**A**

**Detection of Potentially Unwanted Applications**

ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.

**Pick an option before you continue:**

- Enable detection of potentially unwanted applications.
- Disable detection of potentially unwanted applications.

**B**

**Detection of Potentially Unwanted Applications**

ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.

**Pick an option before you continue:**

- Don't detect potentially unwanted applications.
- Detect potentially unwanted applications.

**C**


**Detection of Potentially Unwanted Applications**

ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.

**Pick an option before you continue:**

- Detect potentially unwanted applications.
- Don't detect potentially unwanted applications.

**D**


**Detection of Potentially Unwanted Applications**  [What is a potentially unwanted application?](#)

ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.

**Pick an option before you continue:**

- Disable detection of potentially unwanted applications.
- Enable detection of potentially unwanted applications.

**E**


**Detection of Potentially Unwanted Applications**  [Why do we ask?](#)

ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.

**Pick an option before you continue:**

- Disable detection of potentially unwanted applications.
- Enable detection of potentially unwanted applications.

**F**


**Detection of Potentially Unwanted Applications**  [What is a potentially unwanted application?](#)

**Pick an option before you continue:**

- Disable detection of potentially unwanted applications.
- Enable detection of potentially unwanted applications.

Fig. 2. Variants A-F.

**G**


**Detection of Potentially Unwanted Applications** 

ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.

**Pick an option before you continue:**

- Disable detection of potentially unwanted applications.
- Enable detection of potentially unwanted applications.

**H**

**Detection of Potentially Unwanted Applications** 

ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.

**Pick an option before you continue:**

- Disable detection of potentially unwanted applications.
- Enable detection of potentially unwanted applications.

**I**

**Detection of Potentially Unwanted Applications**

ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.

**For example,** they may change your web browser's webpage and search settings.

**Pick an option before you continue:**

- Disable detection of potentially unwanted applications.
- Enable detection of potentially unwanted applications.

**J**

**Detection of Potentially Unwanted Applications**

**Notice:** ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.

**Pick an option before you continue:**

- Disable detection of potentially unwanted applications.
- Enable detection of potentially unwanted applications.

**K**

**Detection of Potentially Unwanted Applications**

ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can **affect your computer's**:

- performance,
- speed,
- reliability,
- behavior.

They usually require user's consent before installation.

**Pick an option before you continue:**

- Disable detection of potentially unwanted applications.
- Enable detection of potentially unwanted applications.

Fig. 3. Variants G-K.

# The usability canary in the security coal mine: A cognitive framework for evaluation and design of usable authentication solutions

Brian Glass\*, Graeme Jenkinson†, Yuqi Liu\*, M. Angela Sasse\*, and Frank Stajano†

\*University College London

†University of Cambridge

**Abstract**—Over the past 15 years, researchers have identified an increasing number of security mechanisms that are so unusable that the intended users either circumvent them or give up on a service rather than suffer the security. With hindsight, the reasons can be identified easily enough: either the security task itself is too cumbersome and/or time-consuming, or it creates high friction with the users’ primary task. The aim of the research presented here is to equip designers who select and implement security mechanisms with a method for identifying the “best fit” security mechanism at the design stage. Since many usability problems have been identified with authentication, we focus on “best fit” authentication, and present a framework that allows security designers not only to model the workload associated with a particular authentication method, but more importantly to model it in the context of the user’s primary task. We draw on results from cognitive psychology to create a method that allows a designer to understand the impact of a particular authentication method on user productivity and satisfaction. In a validation study using a physical mockup of an airline check-in kiosk, we demonstrate that the model can predict user performance and satisfaction. Furthermore, design experts suggested personalized order recommendations which were similar to our model’s predictions. Our model is the first that supports identification of a holistic fit between the task of user authentication and the context in which it is performed. When applied to new systems, we believe it will help designers understand the usability impact of their security choices and thus develop solutions that maximize both.

## I. INTRODUCTION

Over the past 15 years, the security community has started to acknowledge that security mechanisms are only effective if they are usable: users frustrated by overzealous security measures bypass the security if they can, or switch to a competing system that is easier to use. While an increased awareness of the damage that lack of usability can inflict is a first step, in practice security experts and developers who choose security mechanisms have no way of gauging what the impact of their choice on users will be—and most are not able to call on a human usability expert to do this for them. There are tools for developers to carry out walkthroughs and assessments of a particular solution. The time it will take a user to complete a task can be estimated using the Keystroke Level Modelling (KLM-GOMS) model [17], and an

automated version CogTools [18] provides such a prediction from screen interaction with the tool. This approach, however, has limitations:

- 1) It only supports evaluation and comparison of specified solutions, rather than discovery of the “best” one, and
- 2) it does not take account of the impact that different mental and physical tasks have on subsequent tasks.

In this paper, we contribute and validate an intellectual tool—a design and evaluation framework—that will help designers gain a better understanding of the cost of security, with specific reference to user authentication. Our framework and methodology assesses security mechanisms not in isolation but in the context of the so-called *primary task* that constitutes the user’s true goal. What users really want (primary task) is to check in for a flight or pay a bill, not recall and enter a password or read off and transcribe a one-time code. From the users’ perspective, these are distractions imposed in the name of security, often to manage threats they don’t know exist.

The cost of a given security measure, such as entering a password, is not absolute: it is instead also a function of its relationship to the other components of the primary task. A recent study [24] found that authentication creates a “wall of disruption” in users’ work. This is not only the time spent on the security task, but the knock-on effect of re-starting the primary task after an interruption. Thus, the cost depends not just on how hard the authentication task is in itself but also on when it occurs in the users workflow, on what functions of the brain it loads and on what else the user was meant to be doing before and after.

We draw on results from cognitive psychology to assess the cost of task switching between different activities. Our framework lets designers model the tasks of the intended scenario and the precedence constraints that describe their relationships, and then quantitatively compares alternatives to suggest combinations that minimize the cognitive load and usability cost to the user<sup>1</sup>.

In addition to providing this novel methodology, we present a validation study which verifies the tool’s insights. Using a physical mockup, we test the tool’s optimal (“best”) suggestion against its pessimal (“worst”) suggestion. Moreover, we surveyed a group of professional designers to test our tool’s automatic suggestions against the intuition of human experts.

Permission to freely reproduce all or part of this paper for noncommercial purposes is granted provided that copies bear this notice and the full citation on the first page. Reproduction for commercial purposes is strictly prohibited without the prior written consent of the Internet Society, the first-named author (for reproduction of an entire paper only), and the author’s employer if the paper was prepared within the scope of employment.  
EuroUSEC ’16, 18 July 2016, Darmstadt, Germany  
Copyright 2016 Internet Society, ISBN 1-891562-45-2  
<http://dx.doi.org/10.14722/eurosec.2016.23007>

<sup>1</sup>When our tool, the canary, indicates that the environment has become toxic for the systems users you know it’s time to beat a hasty retreat.

## II. MODELLING A BUSINESS PROCESS

A business process (or workflow) is a collection of interrelated tasks that are performed by users in order to achieve some objective. It is often the case that only authorized users may perform certain tasks: in such cases the business process will include one or more tasks requiring explicit user authentication. Tasks that require authentication impose ordering constraints on the business process (users shouldn't be able to complete a task requiring authorization until they have been authenticated). More generally, the business process may have some freedom in the order in which tasks are performed, that is, the tasks have a partial order. In such cases, system designers have flexibility to rearrange tasks to maximise the system's usability.

Our goal in modelling a business process is twofold. Firstly, we wish to determine the optimal ordering of the tasks, taking into account the switching costs described in sections IV-B and IV-C. Secondly, we wish to explore the impact of equivalent but alternative tasks for user authentication. Thus, our model of a business process must include:

- A representation of the set of steps to be performed,
- A set of tasks that can be performed at each step,
- Hard constraints that enforce the partial ordering of the tasks, and
- Soft constraints that capture the costs of switching between tasks.

### A. Example: airport check-in kiosk

Throughout this paper our example will be airport check-in using a self-service kiosk. We are not modelling the kiosk of any particular airline or airport but an imaginary one that combines features we have observed on a variety of real kiosks. We use this business process as our example because its tasks, listed in Table I, use a range of different cognitive resources, detailed in Table IV. We include cognitive tasks such as making decisions or selections and carrying out checks, as well as physical tasks like attaching luggage tags. The check-in procedure necessarily also includes some form of authentication, but there are multiple ways of achieving that. Helping a designer select the most appropriate authentication mechanism for a specific business process is one of the goals of our framework.

We are also interested in finding the optimal order for the tasks. The check-in kiosk example exhibits a reasonable degree of ordering flexibility. Figure 1 shows the dependencies between the check-in tasks.

## III. OUR FRAMEWORK

The framework we present allows developers to assess the usability of different security tasks within a workflow such as the check-in example described above. Two overarching principles inspired this framework:

- 1) Assessing the usability of an individual task is important, but insufficient, and
- 2) the order in which tasks appear can have an interactive, global effect on overall usability.

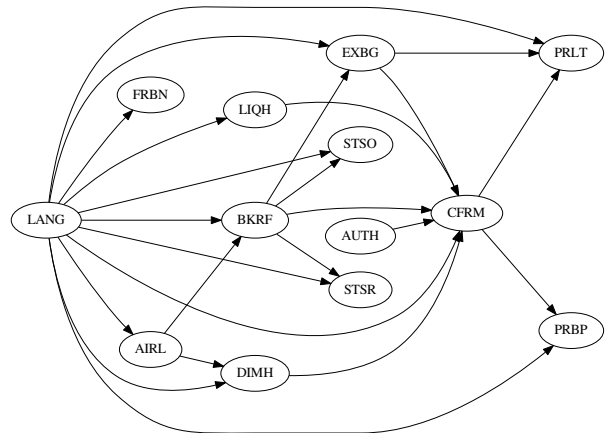


Fig. 1. Dependencies between Airport self-service check-in tasks. An edge from node  $u$  to node  $v$  indicates that  $u$  must be carried out before  $v$ . For example, users must enter their booking reference (BKRf) sometime before they confirm their check-in (CFRM).

Specifically, these principles imply that swapping out one authentication method for another may have carryover effects on the overall workflow. They also suggest that an automated optimization procedure could be used to “solve” for the optimal ordering of tasks—the one that minimises cognitive interruptions and maximizes usability.

A workflow has some number of “steps” and the user can carry out exactly one task at each step. We want to find the optimal assignment of tasks to steps, respecting any ordering constraints between the tasks—ensuring, for example, that certain tasks happen after the authentication task. We will present a method for encoding a workflow as a weighted constraint satisfaction problem (WCSP) [25], in which there are a set of variables (the steps), a set of values (the tasks) and a set of constraints. Further information about constraint satisfaction problems is given in section V and the means of encoding a workflow is explained in section V-B. Workflow environments that are designed to accomplish a specific goal (e.g., withdrawing cash from an ATM, or checking in at an airport kiosk) can be conceptualized as a sequence of tasks completed in a linear fashion. Transitioning from one task to another will carry an additional transition cost. The total usability of an overall task is thus a combination of the costs of the individual tasks and the costs of the pairwise transitions between the tasks in the linearized sequence. Task ordering can have a potentially unpredictable impact on the entire task workflow. Considering the usability of many different potential orderings is a non-trivial task but a computerized tool that computes optimal ordering solutions makes it tractable.

The concept that reordering tasks can have an effect on usability comes from established principles in cognitive psychology. An established literature exists on the relative ordering effects of different types of tasks [20]. In section IV we explain how these effects were operationalized from available literature. In this section, we give an overview of how to extend existing assessments of workload by considering not only the endogenous task demands but also the additional exogenous

Task	Code	Prerequisites	Description
Select language	LANG		User selects their preferred language from the displayed options.
Select airline	AIRL	LANG	User selects their airline from the displayed options.
Booking reference	BKRF	LANG, AIRL	User enters their booking reference using an touchscreen QWERTY keyboard.
<i>Authenticate</i>	<i>AUTH</i>		User authenticates their identity.
▷ Passport scan	AUPS	LANG	User authenticates by scanning the photo page of their passport.
▷ Passport information	AUPI	LANG	User authenticates by manually entering their passport information.
▷ Insert payment card	AUCC	LANG	User authenticates by inserting their payment card.
▷ Password	AUPW	LANG	User authenticates by typing a password (assuming the user has an account with the airline).
Check forbidden items	FRBN	LANG	User presses a button to confirm that their luggage doesn't contain any of the displayed items.
Check liquids	LIQH	LANG	User presses a button to confirm that their hand luggage doesn't contain any containers of liquid above a certain volume.
Check luggage size	DIMH	LANG, AIRL	User presses a button to confirm that their hand luggage is below a certain size.
Select outbound seat	STSO	LANG, BKRF	User selects their outbound seat by clicking on a plan of the available seats in the airplane.
Select return seat	STSR	LANG, BKRF	User selects their return seat by clicking on a plan of the available seats in the airplane.
Buy extra bag	EXBG	LANG, BKRF	User optionally pays for additional luggage by clicking a button and swiping a credit card.
Confirm	CFRM	LANG, BKRF, AUTH, LIQH, DIMH, EXBG	User confirms the details entered so far by reading some text and pressing a button.
Print luggage tag	PRLT	LANG, EXBG, CFRM	User takes a luggage tag from the machine and attaches it to their luggage.
Print boarding pass	PRBP	LANG, CFRM	User takes a boarding pass from the machine.

TABLE I. AIRPORT SELF-SERVICE CHECK-IN TASKS.

demands that emerge from the transitional costs between tasks.

#### A. Completion times

Various methods have been devised to predict the time required to complete a given task. A popular technique is KLM-GOMS [17]. In this technique, the designer breaks down the task into a variety of individual action components (for example: mentally prepare, click button, press a key), each of which has an associated reaction time. This technique is useful for estimating how long it would take a user to complete a given task. Another assessment technique is CogTool [18], which assesses task completion times and learning rates based on shifting visual attention and making motor responses. Both methods use approximations for mental processes (*think* in CogTool, *mental preparation* in KLM-GOMS). In the present paper, we seek to expand on these techniques by assessing the differential cognitive demands of different tasks as well as task transitions.

#### B. Cognitive demands of tasks

While subjective measures of workload are useful tools in predicting user satisfaction and adoption rates, the operationalization of workload as a unitary resource does not fit with modern theories of cognition [10], [11]. Rather, a variety of dissociable mechanisms underlie cognition and become active given characteristics of the task at hand [3]. In section IV-B2 we address the various cognitive mechanisms involved in an individual task.

#### C. Cognitive demands of transitions

While tasks carry their own demands, there are also certain performance costs associated with switching from one task to another. These transitional costs can be asymmetric; that is, switching from Task A to Task B may be more costly than switching from Task B to Task A [20]. For this reason, we have coded principles of task switching costs from existing literature. In section IV-B and section IV-C we address the various types of switch costs used in the present modelling procedure.

#### D. Quantifying tasks

The goal of our work is to promote a discipline for considering both the unary and transitional demands of tasks on users, and to demonstrate a method for improving performance by minimizing overall task demand. The effectiveness of any given instantiation of this methodology depends directly on the quality of input information about the workflow being analysed. Thus, it will be crucial to develop a valid and reliable regimen for quantifying task characteristics. In this initial paper we are charting a new path and, for illustrative purposes, we have assigned numerical values based on our judgement. In future work we would develop instruments such as worksheets and flowcharts to help independent designers assign consistent and reproducible numerical values when they assess their tasks.

### IV. COGNITIVE PSYCHOLOGY

#### A. Task switching

When a person switches from one task to another task, the brain must reorganize and reallocate cognitive resources to ensure an efficient transition [20]. Transitioning from a task that primarily uses resource *A* to a task that primarily uses resource *B* (instead of continuing to use resource *A*) results in performance deficits, or switch costs. Experimental psychology has uncovered certain principles that govern these transitions. These so-called *switch cost asymmetries* have been shown to occur, or not, depending on other characteristics of the tasks involved. We have codified these task asymmetries (expressed as Cohens *d* effect sizes, which are a commonly used metric in psychology for comparing the mean of one sample to that of another [13]) into a collection of rules that may be encoded as constraints in a weighted constraint satisfaction problem (see section V). Below, we describe how we constructed these rules from available literature on switch cost asymmetries. The rules fall into two categories: *cognitive resource transitions* and *task property transitions*.

#### B. Cognitive resource transitions

One reason that task switching results in a performance deficit is the requirement for the individual to disengage active cognitive mechanisms and then engage other cognitive mechanisms in order to match task demands [20]. For example,

switching from a visual task to an auditory task is more costly than vice versa [28]. In a practical example, if a person were performing a hypothetical two-factor authentication procedure that involved recognizing an image among several on a large screen and also recognizing a voice over a phone line, it could be more efficient to place the audio identification subtask before the visual authentication subtask. This demonstrates that task ordering can impact user efficiency due to asymmetries in cognitive switch costs.

1) *Cognitive resources demands of individual subtasks:*

The cognitive mechanisms included in the present implementation are visual working memory (VWM; responsible for holding, processing, and operating on information of immediate importance), procedural memory (PM; responsible for storing and preparing motor action sequences), declarative recall (DR; responsible for generating and presenting stored information on demand), semantic recognition (SR; responsible for determining whether factual information has been stored in memory), and episodic recognition (ER, responsible for determining whether information about experienced events have been stored in memory). Note that while the categories represented here have an empirical basis, the taxonomy of mental processes is a fluid research topic [4].

Table II reports the costs of switching between tasks utilising different cognitive mechanisms. The values are Cohen’s *d* effect sizes and were calculated from published studies [13] involving empirical measurements of reaction time in various task switch contexts, which assessed the efficiency with which individuals were able to transition between different cognitive systems.

2) *Operationalizing the check-in task:* In order to utilise these principles of task switch cost asymmetry, we operationalised identified the cognitive resources most likely to be engaged by the subtasks involved in the Airline Self-Service Task. While this is a first approximation, in the future empirical methods could be used to verify these predictions. In real-world tasks, many different cognitive mechanisms are likely to be engaged simultaneously. For our purposes, we have selected the dominant resource which is predicted to have the highest relative engagement level. Table IV reports the major cognitive resource assigned to each subtask, as well as the physical response modality, voluntary/involuntary nature, task familiarity, and task complexity.

It is impractical to determine the specific brain networks activated for a specific real task, so we characterize each task by assessing its similarity to documented cognitive tasks. For example, determining whether a piece of hand luggage exceeds certain dimensions is similar to documented tasks involving assessing geometric attributes of three dimensional shapes, a task known to activate visual working memory [12]. This is a tractable simplification of the reality of cognitive functioning for two reasons:

- 1) Real-world tasks likely engage many different cognitive mechanisms at once, with varying degrees of demand. For our purposes we consider the cognitive mechanisms deemed to be most relied upon in order to complete the task.
- 2) Many other cognitive mechanisms exist than were included in Table II. For simplicity, we only included

the primary mechanisms involved for each task. Future implementations could include other systems such as auditory working memory.

C. *Task property transitions*

An important source of task switch costs is the impact of the interference or inertia carried over from one to another. One counterintuitive finding is that switching from a less familiar task to a more familiar task is actually more disruptive than vice versa [29]. The prevailing reasoning behind this effect is that when engaged in a less familiar task, the individual must suppress commonly used mental processes in lieu of less frequently used processes [14]. This suppression has a carry-over effect on the new task, resulting in a performance deficit. These transitional asymmetries have also been identified when transitioning between tasks that differ by complexity [22], recent practice [29], modality (form or method of response) [23], and whether the task was voluntary [2]. These empirical observations have been codified into conditional rules with associated effect sizes in Table III.

1) *Complexity:* Task complexity was assessed using existing definitions from experimental psychology [22], namely the number and combination of rules required to solve or complete the task. For example, subtraction is relatively less complex than division. The reason for this is that division uses the principles of subtraction as well as other principles, such as remainders and carrying digits between places. In the airline check-in task, for example, the task regarding forbidden materials was considered to be more complex than the task regarding liquids. This is because it is more complex to determine whether several items fall into several categories versus a single category.

2) *Familiarity:* Task familiarity was determined by assessing not only the frequency with which an average user completes a given task, but also whether the task assesses familiar knowledge or processes [29]. For example, selecting your language preference might not necessarily be a common chore, but it requires judgment based on a familiar fact. In contrast, printing a luggage tag is something that is an activity that is both infrequent and unfamiliar.

3) *Response Modality:* Response modality refers to the physical method for issuing a response from the user to the system. For example, different modalities include a QWERTY keyboard, a mouse pointer, or a verbal response. There is evidence that transitioning from one response modality to another can incur a switch cost. However, Sandhu and Dyson [23] demonstrate that a switch cost due to response modality may not occur when a modality switch coincides with a cognitive resource switch. In other words, switching response modalities is most disruptive when it is the only change that takes place.

V. MODELLING A BUSINESS PROCESS AS A CONSTRAINT SATISFACTION PROBLEM

A. *Constraint satisfaction problems*

The goal of a constraint satisfaction problem (CSP) is to assign *values* to a set of *variables* subject to a set of *constraints*. The constraints express *local* restrictions, such as

		To				
		VWM	PWM	DR	SR	ER
From	Visual working memory (VWM)	0	0.495	0.495	0.495	0.157
	Procedural memory (PM)	0.495	0	0.495	0.699	0.699
	Declarative recall (DR)	0.495	0.495	0	0.482	0.482
	Semantic recognition (SR)	0.495	0.842	1.078	0	0.433
	Episodic recognition (ER)	0.307	0.842	1.078	0.354	0

TABLE II. COSTS OF SWITCHING BETWEEN TASKS UTILISING DIFFERENT COGNITIVE MECHANISMS, GIVEN AS COHENS  $d$  EFFECT SIZES.

Rule name	Condition	Cost (effect size)
Modality	A switch occurred which uses the same resources (on-diagonal above) <b>and</b> there is a modality switch.	0.16
Recent Practice	A task of similar modality or resource has been used anywhere previously.	0.31
Familiarity	The current task is more familiar than the previous task.	0.42
Complexity/Choice	A task is done voluntarily <b>and</b> the complexity decreases.	2.92
	A task is involuntary <b>and</b> the complexity decreases.	1.63

TABLE III. ADDITIONAL COSTS OF TRANSITIONING BETWEEN TASKS DETERMINED BY SPECIFIC RULES, GIVEN AS COHENS  $d$  EFFECT SIZES.

Code	Primary cognitive resource	Modality	Voluntary?	Familiarity	Complexity
LANG	Semantic recognition	Touchscreen	No	5	1
AIRL	Episodic recognition	Touchscreen	No	5	1
BKRF	Visual working memory	Touchscreen QWERTY	No	3	3
AUPS	Procedural memory	Passport scanner	No	2	2
AUPI	Procedural memory	Touchscreen QWERTY	No	2	3
AUCC	Procedural memory	Credit card reader	No	3	2
AUPW	Declarative recall	Touchscreen QWERTY	No	4	3
FRBN	Semantic recognition	Touchscreen	No	2	3
LIQH	Episodic	Touchscreen	No	3	3
DIMH	Visual working memory	Touchscreen	No	2	4
STSO	Visual working memory	Touchscreen	Yes	2	4
STSR	Visual working memory	Touchscreen	Yes	2	4
EXBG	Episodic	Touchscreen	Yes	2	2
CFRM	Episodic	Touchscreen	No	4	2
PRLT	Procedural memory	Luggage tag	No	1	5
PRBP	Episodic	Touchscreen	Yes	4	2

TABLE IV. PROPERTIES OF THE CHECK-IN KIOSK TASKS. FAMILIARITY AND COMPLEXITY ARE ON A SCALE FROM 1 (LOW) TO 5 (HIGH).

“these two variables must have different values”. An evaluation of the CSP is consistent and complete if it includes all variables and does not violate any constraints (efficient algorithms for finding global solutions are given in [21]). Below we shall describe *weighted* constraint satisfaction problems: these include “soft” constraints that may be violated for some cost. We first introduce the classic CSP framework.

1) *Classic CSP*: A *classic* CSP is defined by a triple  $P = (X, D, C)$ .  $X$  is the set of variables,  $\{x_1, \dots, x_n\}$ . A domain  $d_i \in D$  is a set of allowable values for variable  $x_i$ . A constraint  $c \in C$  is a pair  $(X_c, R_c)$ , where  $X_c \subset X$  is the *scope* of the constraint and  $R_c$  is a relation over the corresponding set of domains.  $R_c$  specifies tuples of simultaneously-allowed values for the variables in the scope and can be defined explicitly as a subset of the product of the domains, or as an abstract relation which can test whether a given tuple of values is allowed, for example:  $x_1 \neq x_2$ .

An *assignment* specifies values for some or all of the variables. An assignment is *consistent* if it does not violate any constraints. A *complete* assignment is one which assigns values to all variables. A *solution* to a CSP is a complete consistent assignment. A CSP is consistent if a solution for it exists. Finding a solution to a CSP is an NP-complete problem.

2) *Weighted CSP*: In a classical CSP the constraints are all absolute or “hard”, no consistent assignment can violate any constraint and all solutions are equally “good”. Several variants have been proposed to extend the CSP framework to include “soft” constraints expressing priorities, preferences, costs, and probabilities. Schiex, Fargier and Verfaillie [25] generalised these and defined *valued CSP* (VCSP). A VCSP is similar

to a classical CSP except that the constraints assign *costs* to assignments instead of allowing or disallowing them<sup>2</sup>.

A VCSP is defined by a tuple  $P = (S, X, D, C)$ , where  $X$  and  $D$  are sets of variables and their domains as previously. Costs are specified using a *valuation structure*, which is a triple  $S = (E, \oplus, \succ)$ , where  $E$  is a set of costs ordered by  $\succ$  and  $\oplus$  is an associative commutative monotonic binary operation on  $E$  for combining costs.<sup>3</sup> Weighted CSP (WCSP) is a specific subclass of valued CSP in which the costs are the natural numbers or positive infinity,  $E = \mathbb{N} \cup \{\infty\}$  and  $\oplus$  is the standard sum operation.

In this framework, constraints specify local costs of assignments. A constraint  $c \in C$  is a pair  $(X_c, F_c)$  where  $X_c$  is its scope and  $F_c$  is a cost function,

$$F_c : \prod_{x_i \in X_c} d_i \rightarrow E \quad (1)$$

Note that a hard CSP constraint  $c = (X_c, R_c)$  can be represented in a WCSP as  $c' = (X_c, F_{c'})$ , where

$$F_{c'}(v) = \begin{cases} 0 & \text{if } v \in R_c \\ \infty & \text{otherwise} \end{cases} \quad (2)$$

<sup>2</sup>Equivalently a VCSP can be seen as classic CSP in which each constraint has been annotated with a cost for removing it [25].

<sup>3</sup>A classical CSP can be expressed as a VCSP with  $E = \{t, f\}$ ,  $\perp = t \succ f = \top$  and  $\oplus = \wedge$ .



Given a WCSP  $P = (S, X, D, C)$ , an assignment  $A$  of variables  $Y \subset X$  has total cost  $V_P(A) \in E$ . This cost is the sum of all applicable cost functions.

Given a WCSP, the typical task is to find the optimal solution, the complete assignment with the minimum total cost. The most popular algorithms for solving WCSP employ branch and bound search, although algorithms for solving WSCP remain an active research area.

## B. Our model

As described in section V-A2, a weighted CSP is represented by the tuple  $P = (S, X, D, C)$ . In our model, a business process with  $n$  steps (where 1 is the first step performed by the user and  $n$  the last) is represented by a set of variables  $X$ ,  $\{x_1, \dots, x_n\}$ . The domain  $D$  (the set of values that can be assigned to variable  $x_i$ ) consists of all of the tasks, including any user authentication tasks, in the business process. The set of constraints  $C$  includes hard constraints that ensure tasks are performed exactly once and ordering relations between tasks are maintained.  $C$  also includes soft constraints represent the costs of switching between tasks.

1) *Implementation of our model:* A proof-of-concept implementation of our model has been created in Numberjack, a Python framework for constraint programming, mixed integer programming and satisfiability solvers [15]. Numberjack integrates a number of third-party, open source solvers (which are typically written in C/C++ for efficiency) and can be easily extended to include additional solvers. The Numberjack framework includes support for Toulbar2—an exact combinatorial optimization tool designed for solving Weighted Constraint Satisfaction Problems (otherwise known as Cost Function Networks) [1]. Numberjack’s proposition of a high-level modelling framework and an underlying efficient and high-pedigree solver<sup>4</sup> make it well suited to our purpose.

As shown below, a Numberjack `VarArray` is used to represent each step in the business process. The domain of each variable is the natural numbers  $0 \dots d$  where each value represents one of the possible tasks. A constraint is then added to the model to ensure that each value in the domain is assigned to exactly one variable.

```
from Numberjack import VarArray

# Create a variable array,
# one variable for each step
# in the business process
wvspVars = VarArray(0, d, nSteps)

model.add(AllDiff(wvspVariables))
```

A custom Numberjack constraint has been created to enforce the partial ordering of tasks. This constraint (shown below) ensures that for all combinations of the variables in the CSP it is never the case that the value *after* is assigned to a variable that precedes a variable assigned the value *before*.

```
class Order(Predicate):
```

```
def __init__(self, vars, before, after):
    Predicate.__init__(self, vars,
        "Order")
    self.set_children(vars)
    self.before = before
    self.after = after
    self.lb = None
    self.ub = None

def decompose(self):
    return [(x != self.after) | (y !=
        self.before) for x, y in
        combinations(self.children, 2)]
```

As defined in section V-A2, a constraint  $c \in C$  is a pair  $(X_c, F_c)$  where  $X_c$  is its scope and  $F_c$  is a cost function. Task switching costs are modelled as binary constraints; that is, their scope is limited to variables that are immediately next to each other. The task switching costs are represented by a  $d$ -by- $d$  matrix (where  $d = |D|$ ).

```
from Numberjack import PostBinary

def pairwise(iterable):
    a, b = tee(iterable)
    next(b, None)
    return izip(a, b)

# d-by-d matrix,
# binaryCost[d1][d2] specifies the
# cost of assigning d1 and d2 to
# variables that are immediately
# next to each other
binaryCosts = [...]

for var, varNext in pairwise(wvspVars):
    model.add(PostBinary(var, varNext,
        binaryCosts))
```

## 2) Results of modelling the airline self service check-in.

Table V shows the optimal task ordering given by the solver for the self-service check-in scenario. The four columns of the table correspond to the four different concrete authentication tasks we are considering. The cost reported for each workflow is the sum of all the task switch costs (Cohen’s  $d$  effect sizes) for that workflow<sup>5</sup>. The fact that the four orderings and total costs are different supports the central message of this paper: fitting an authentication task to its context is important. Specifically, we can see that the passport scan (AUPS) and insert payment card (AUCC) authentication methods yield substantially lower total switching costs—*regardless* of their intrinsic costs. More generally, with twelve task switches in total, the mean cost for each task switch, in each of the four cases, is approximately 0.5, which constitutes a “medium” effect size under the standard Cohen’s  $d$  interpretation: this indicates that task switches are not an insignificant cost in general.

It is interesting to note that the solver splits the two seat selection tasks for the outgoing and return flight. Within the model, the two selection tasks are indistinguishable so the cost

<sup>4</sup>Toulbar2 was a winning solver in the Uncertainty in Artificial Intelligence (UAI) 2010 Approximate Inference Challenge.

<sup>5</sup>To obtain the total cost, we should add to that the costs of the individual subtasks. We cannot do that yet, because they are expressed in different non-comparable units, so this is a topic for future research. See the next section, V-B3.

Select language	Select language	Select language	Select language
Select airline	Select airline	Select airline	Select airline
Check liquids	Check liquids	Check liquids	Check liquids
Booking reference	Booking reference	Booking reference	Booking reference
Check forbidden items	<b>Insert payment card</b>	<b>Passport info</b>	<b>Password</b>
Select return seat	Buy extra bag	Select return seat	Check forbidden items
Check luggage size	Select return seat	Check luggage size	Select outbound seat
<b>Passport scan</b>	Check luggage size	Check forbidden items	Check luggage size
Buy extra bag	Check forbidden items	Buy extra bag	Buy extra bag
Confirm	Confirm	Confirm	Confirm
Print boarding pass	Print boarding pass	Print boarding pass	Print boarding pass
Select outbound seat	Select outbound seat	Select outbound seat	Select return seat
Print luggage tag	Print luggage tag	Print luggage tag	Print luggage tag
Cost 5.53	5.88	8.18	8.42

TABLE V. OPTIMAL TASK ORDERING OF THE SELF-SERVICE CHECK-IN USING DIFFERENT AUTHENTICATION MECHANISMS.

of switching from either to the other is zero. Therefore, we might expect that the solver would place these task next to each other. However, this is an interesting example of how our intuition can be wrong as this local optimization ultimately precludes the globally optimal solution.

### 3) Limitations of our model:

Essentially, all models are wrong, but some are useful.  
—George E. P. Box [6]

The first significant limitation of our model is its inability to relate the reported total task switching costs to an additional amount of *time* required to complete the business process. Whilst this is a significant limitation, we feel that the outputs of the model remain useful and may be used alongside the existing techniques for estimating the time taken to carry out specific tasks such as KLM-GOMS.

Secondly, although the cognitive resource transition costs and task property transition costs are based on empirical results from the literature, user studies should be undertaken to validate the way in which they combine within our framework.

As well as splitting up the two seat selection tasks, in three cases the solver has placed return seat selection before outbound seat selection. While this would obviously be somewhat confusing for users, it is understandable that the solver has arranged the tasks in this way because within the model they appear identical. Our model simply doesn't capture the notion that when tasks relate to events that are ordered, it makes sense for those tasks to have the same order. In such cases the system designer must apply their discretion to ensure that the system remains consistent with reality and with user expectations.

## VI. VALIDATION STUDY

In order to test the model's predictions, we completed a validation study. Our intention was to validate the theoretical predictions regarding task switching, and thus we focused on the subtasks which would be inherent in airline check-in kiosks regardless of further authentication mechanisms used (e.g., credit card, passport). Using a mock-up of the airline check-in kiosk described above, we sought to assess the model's optimal subtask ordering recommendation. We accomplished this in four ways: 1) Participants completed the optimal ("best") ordering in a simulated airline departure scenario, 2) These same participants offered their own order recommendations for the task, 3) We further tested a second sample of participants with the pessimal ("worst") ordering, and 4) We surveyed professionals trained in design fields in

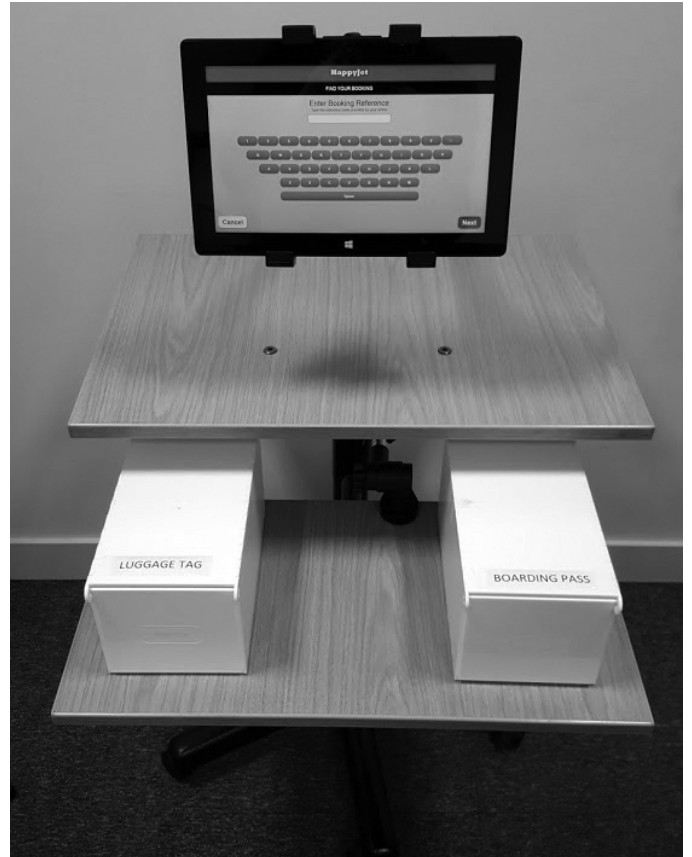


Fig. 2. Mock up for the self-service airport check-in kiosk.

order to gather an expert based ordering recommendation. The Optimal ordering was: AIRL, LIQH, BKRF, FRBN, STSO, DIMH, EXBG, CFRM, PRBP, PRLT; the Pessimal ordering was: FRBN, AIRL, BKRF, EXBG, LIQH, DIMH, CFRM, PRLT, STSO, PRBP.

### A. Participants

Participants were recruited from the University College London student and staff community and compensated £7 for their time. The study was approved by the UCL Ethics Committee, and all participants offered informed consent. For the Optimal condition, 40 participants were recruited. A sample of 20 participants was recruited for the comparative Pessimal condition, and a further 50 self-reported design professionals were recruited to generate the Expert ordering suggestion. The

demographics of the group were as follows: Optimal group ( $Age_{Mean} = 26.6$ ,  $Age_{SD} = 7.2$ , 28 females), Pessimist group ( $Age_{Mean} = 29.1$ ,  $Age_{SD} = 13.5$ , 15 females), Expert designers ( $Age_{Mean} = 30.0$ ,  $Age_{SD} = 9.7$ , 12 females, 8 no gender specified). Two participants were removed from the Optimal group for not completing the task, and three were removed from the Expert group for not completing the survey. Participants were asked about their average annual number of flights:  $OptimalGroup = 4.7(SD = 3.4)$ ,  $PessimistGroup = 3.5(SD = 3.2)$ .

The sample of Expert designers was recruited from NCR Corporation ([www.ncr.com](http://www.ncr.com)) as well as via the online survey system Prolific Academic ([www.prolific.ac](http://www.prolific.ac)), and were selected using a pre-screening occupation questionnaire. The group identified as working with user experience design in physical settings ( $n=17$ ), software/web settings ( $n=33$ ), or both ( $n=6$ ), with 5.2 mean years of experience ( $SD = 6.0$ ). These participants were compensated with £1.67 for completing the task (equivalent to £5/hour).

## B. Procedure

1) *Check-in Kiosk*: Participants were asked to use the simulated airline check-in kiosk as if they were actually preparing for a departure at an airport. Participants were given two suitcases, one large suitcase for checked baggage, and one small suitcase for carry on. The experimenter opened the small suitcase and described the contents to the user: two shirts, two paperback books, and a plastic bag containing toiletries under 100ml in volume. The experimenter told the participant that the large suitcase contained clothes and no hazardous or forbidden materials. The participants completed the airline check-in kiosk three times, each time with a different provided cover story (given in pseudo-random order between participants). The mock airlines were “MetroAir”, “HappyJet”, and “QuickFly”, and the mock destinations were Glasgow, Edinburgh, and Cardiff (departing from London). Participants took the two suitcases and entered a second room to interact with a kiosk comprised of a touchscreen monitor and two dispensers (one for boarding pass, one for baggage tag) on a small roller table (see Figure 2). The flapped dispensers were pre-loaded with the relevant boarding pass and baggage tag, and a simulated printing sound oriented the participant to their locations during the appropriate subtask. After completing each of the three simulated check-in procedures, the participant moved to a different room and completed the subjective satisfaction questionnaire.

2) *Subjective Satisfaction Questionnaire*: After each trial, participants completed the following 13-item Satisfaction Questionnaire [8]. Each item was scored using a 5-point Likert scale (from “Strongly disagree” to “Strongly agree”). In order to reduce repetitiveness, the second and third repetitions of the questionnaire asked for changes in assessment relative to the previous trial (from “Less than before” to “More than before”). In this way, a change score was computed using responses from the first trial as a baseline.

- 1) The system was annoying to use.
- 2) I liked using the system.
- 3) The system did what I thought it would do.
- 4) The system was fun to use.

- 5) The system was unreliable.
- 6) I was satisfied using this system.
- 7) I was comfortable using this system.
- 8) The system was disappointing.
- 9) The system was engaging.
- 10) The system was unpredictable.
- 11) I feel positive about the system.
- 12) I would not want to use this system.
- 13) The system was pleasant to use.

3) *Ordering Preference Task*: After the completion of the check-in procedure, participants were asked to generate their own suggested orderings for the subtasks. Using a computerized tool, participants dragged boxes representing the various subtasks into their preferred orderings. First, participants were allowed to freely order the subtasks without partial ordering constraints. Second, participants were told which subtasks violated the partial ordering constraints (if any), and were asked to rearrange the subtasks until the ordering satisfied the constraints (see Figure 6).

## C. Results

1) *User Performance*: Task performance was measured by calculating the time to complete each subtask. The time was computed based on the duration from completion of previous subtask to the completion of the current subtask. Results were similar when time was calculated as the duration from the completion of the previous subtask to the first click of the current subtask, although some subtasks only required one click, thus we present subtask completion times here.

To evaluate the impact of our model’s ordering suggestions as well as the impact of prior kiosk experience, participants were further clustered into two experience groups: Have used airline check-in kiosk in the previous calendar year (Used Kiosk), or have not (No Kiosk). Learning curve (repetition over the three trials) was also evaluated as a within subjects factor. Performance (mean completion time) was evaluated using a repeated measures ANOVA with a 2 (Condition: Optimal, Pessimist) x 2 (Experience: Used Kiosk, No Kiosk) x 3 (Repetition) factorial design. There were significant main effects of Condition ( $F_{1,55} = 4.82, p = 0.03$ ) and Experience ( $F_{1,55} = 5.01, p = 0.03$ ) such that those in the Optimal order had faster completion times, and those with airline kiosk experience in the previous year had faster completion times. There was a significant main effect of Repetition ( $F_{2,110} = 81.0, p < 0.001$ ) consistent with a monotonic learning curve (see Figure 3). There was also a significant interaction of Repetition and Experience ( $F_{2,110} = 5.09, p = 0.01$ ) such that those with experience demonstrated a flatter learning curve due to faster initial completion times (see Figure 4). Completion time was lower for 8 out of 10 subtasks (essentially tied for PRBP and AIRL). According to the binomial distribution, the probability of a result at least this extreme occurring from randomly generated data is 5.3%. In summary, those in the Optimal ordering condition demonstrated faster completion times on all three repetitions of the task, and those with prior experience were overall faster as well.

2) *User Satisfaction*: User satisfaction was measured using the 13-item Satisfaction Questionnaire (see above) by taking the average responses on a 5-point Likert scale (reverse coded

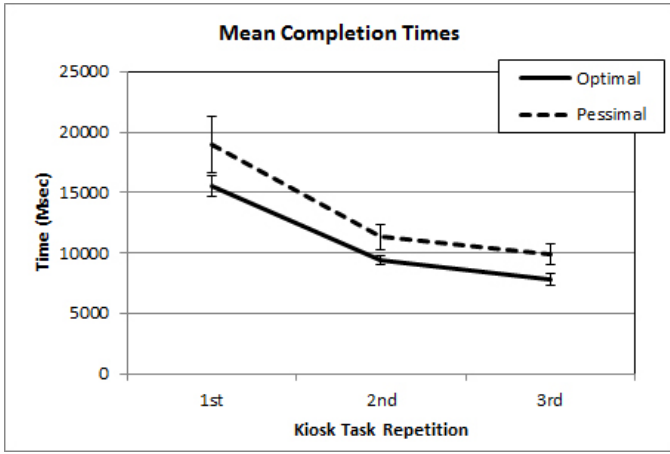


Fig. 3. Mean completion times over three task repetitions between Optimal ordering and Pessimal ordering conditions.

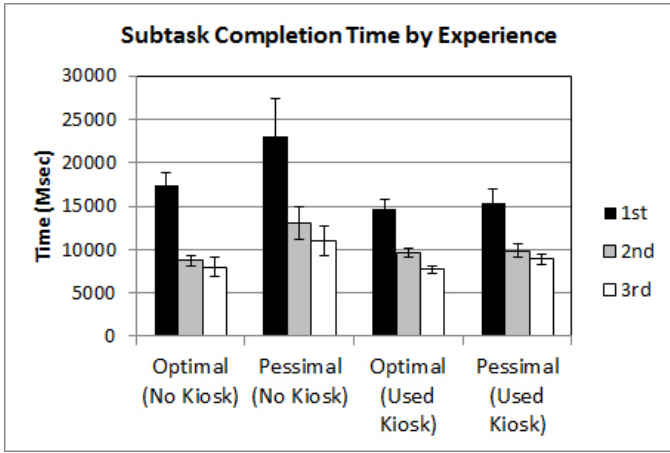


Fig. 4. Mean completion times over three task repetitions between Optimal ordering and Pessimal ordering conditions, by experience.

for the negatively worded items). For the second and third completion of the questionnaire, the scores were demeaned (subtracted by 3) and added to the previous questionnaire’s result. Satisfaction was evaluated using a repeated measures ANOVA with a 2 (Condition: Optimal, Pessimal) x 2 (Experience: Used Kiosk, No Kiosk) x 3 (Repetition) factorial design. Although directionally in favor of the Optimal ordering, the satisfaction ratings were not statistically significantly higher for the Optimal ordering versus the Pessimal ordering ( $F_{1,55} = 2.15, p = 0.149$ ). There was a significant main effect of Repetition ( $F_{2,110} = 27.9, p < 0.001$ ) such that subjective user satisfaction increased monotonically over the three task repetitions. There was a significant three-way interaction of Repetition, Condition, and Experience ( $F_{2,110} = 3.68, p = 0.03$ ). Figure 5 illustrates the nature of this interaction, such that those with no kiosk experience were more sensitive to the Optimal vs. Pessimal manipulation than those with kiosk experience. Specifically, those with no kiosk usage in the previous year found the Optimal ordering to be more satisfactory over time relative to the Pessimal ordering.

3) *Ordering Preferences*: Participants provided their own recommended orderings for the kiosk subtasks. Separately,

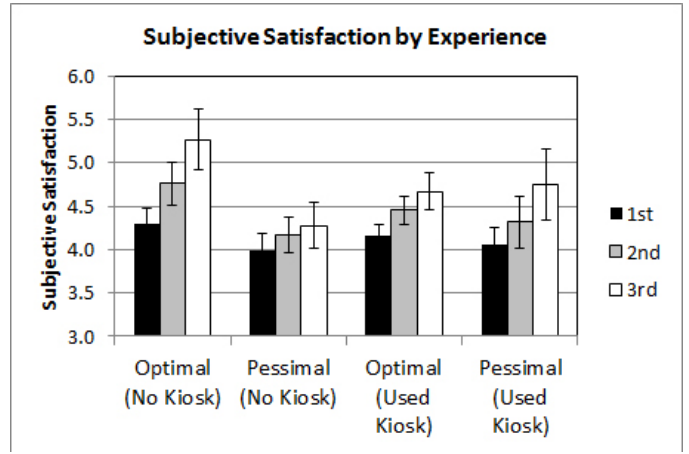


Fig. 5. Satisfaction Scores over three task repetitions between Optimal ordering and Pessimal ordering conditions, by experience.

self-reported design professionals (who did not complete the kiosk task) also provided recommended orderings. From these experts, a consensus Expert ordering was generated (AIRL, BKRF, STSO, DIMH, FRBN, LIQH, EXBG, CFRM, PRLT, PRBP) using the mode frequencies from each subtask index. A Euclidean distance metric (based on index differences) was computed for each participant’s recommended ordering. In this way, we were able to calculate a participant’s suggestion’s difference from the model’s Optimal ordering, Pessimal ordering, and an Expert ordering. The Expert ordering was significantly more similar to the model’s Optimal ordering than the Pessimal ordering ( $t_{Paired} = 9.15, p < 0.001$ ). Thus, Experts suggested orderings which were more similar to the model’s Optimal suggestion.

Preferred ordering was evaluated using a repeated measures ANOVA with a 2 (Condition: Optimal, Pessimal) x 2 (Experience: Used Kiosk, No Kiosk) x 3 (Comparison Source: Optimal, Pessimal, Expert) factorial design. There was a significant main effect of Comparison Source ( $F_{2,110} = 27.4, p < 0.001$ ) and a significant interaction of Comparison Source and Condition ( $F_{2,110} = 7.92, p = 0.001$ ) such that those who participated in the Optimal ordering gave suggestions which were more similar to both our Optimal ordering and the Expert ordering. In summary, the Expert suggested order and the model’s Optimal suggested order were closer to recommendations given by participants who had experienced the Optimal ordering (see Figure 7).

## VII. CONCLUSION AND FURTHER WORK

We presented a framework for reasoning about the impact of user authentication on the overall usability of a workflow. Our framework is the first to highlight the importance of the fit between a particular user authentication method and the context in which it is performed. Specifically, we draw on results from cognitive psychology to quantify the impact of switching between tasks that draw on different cognitive resources and use different modalities.

This is a new, disruptive approach to evaluating usability of security solutions, and even systems usability in general. We are sharing this powerful core idea with the community in

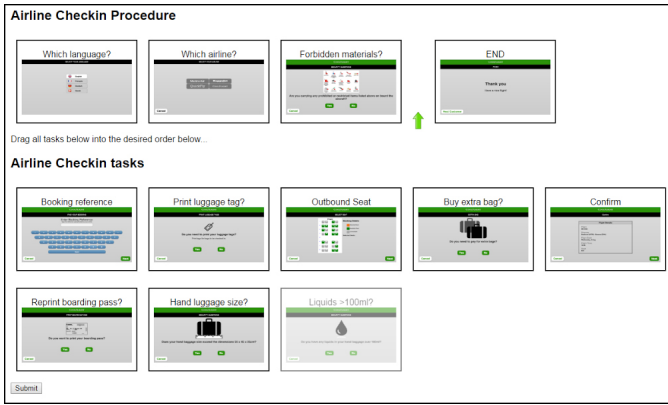


Fig. 6. Screenshot of the ordering preference task.

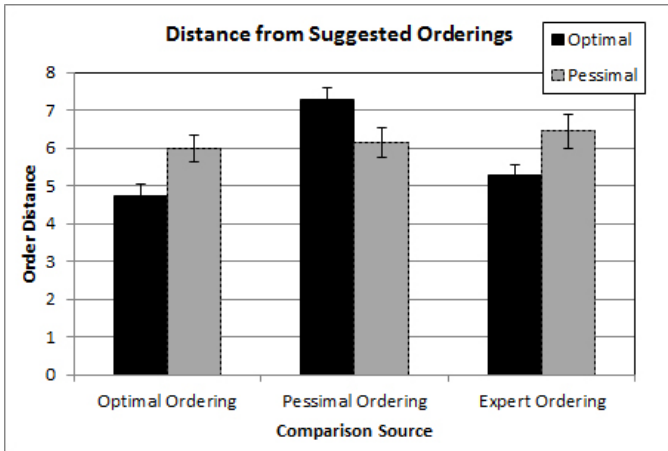


Fig. 7. Difference of participants’ suggested orderings to the model’s Optimal and Pessimal ordering, as well as an Expert suggested ordering.

its preliminary form but we envisage further work in several directions, both on our proof-of-concept implementation of the solver and on the framework itself. We need to develop reliable input tools, such as worksheets and flowcharts, to allow independent designers to perform consistent assignment of numerical values to the features of their tasks. More fundamentally, we would like to develop a “unit” (not necessarily just elapsed time; maybe other factors like stress and annoyance might come into it) to measure the usability cost, and a disciplined and justifiable method for expressing in this same unit both the cost of a task and the additional cost of a transition. This will allow the CSP solver to add those sub-costs to compute a globally optimal solution. These additional steps go hand in hand with user studies and validation of the modelling approach. But the general principles and methods that underlie our framework are already useful and applicable today.

Our framework targets two audiences: designers of secure systems and designers of new authentication schemes. System designers can use the framework as scaffolding that supports the overall design process. This scaffolding encourages the designer to think about how their use of authentication is likely to impact on their users and ultimately on the success of the system. Similarly, security researchers developing new authentication primitives can use the framework to reason

about their solution within a realistic context of use.

Importantly, the theoretical model output was further validated with a user study. Participants performed better in the optimal ordering, and were more satisfied by the optimally ordered interface. The model’s optimal ordering was more similar to the suggested orderings of professional designers, and participants who experienced in the optimal ordering were more likely to further prefer and recommend such an ordering. In this way, we were able to validate the predictions of the theoretical model.

The consolidation of results from cognitive psychology on the effects of task switching, and the presentation of these results in a format directly usable by security professionals is perhaps the most useful contribution of our work.

## VIII. RELATED WORK

Sasse *et al.* [24], [27] present their findings of a 2-part study into the impact of authentication on the productivity of employees in a US governmental organisation. They conclude that the overall burden of user authentication includes a disruption to the user’s primary task (that is, what they are actually trying to achieve). Disruptions resulting from user authentication damage productivity and result in significant frustrations. Furthermore the authors found that *avoidance*—not logging into services or using them less frequently—was an increasingly common coping strategy when the burden of authentication was felt to be too great.

While Shay *et al.* [26] have attempted to boost security by pushing the limits of user workload, there is a call for designers to consider the impacts of effortful authentication mechanisms on the user. Employees reported to Inglesant and Sasse [16] that they’d resort to insecure workarounds in response to increasingly stringent password policies. This friction [5] between the tasks has been shown to moderate individual compliance.

Building on these observations, our work is the first attempt to develop a model of such costs. The ultimate goal of this model is to empower system designers to reason about such effects before deployment.

Prior work has demonstrated the usefulness of modelling subtask arrangement to find optimal orderings. Crampton [9] arranges security-related subtasks to find orderings that satisfy entailment, cardinality, and role-based constraints. Zhang *et al.* [30] use an optimization procedure to minimize mouse clicks in a computerized task workflow. Our methodology uses similar techniques to consider a finer grained user-centric cost model to optimize the handing off of cognitive mechanisms throughout a task.

Constraint Satisfaction Problems (CSP) have long found application in decision supports systems. Scheduling—determining the optimum allocation of shared resources to competing activities—is a well-known NP-complete Constraint Satisfaction Problem (CSP) [19].

Cohen *et al.* [7] apply techniques from CSP to the *Workflow Satisfiability Problem (WSP)*—that is, deciding whether a plan exists for assigning task to authorized users in a given business process. Our work draws inspiration from their use

of CSP. However, in our framework we are concerned with an optimization problem.

#### ACKNOWLEDGMENT

The Cambridge authors are grateful to the European Research Council for funding this research through grant StG 307224 (Pico). The UCL authors are grateful to the Engineering and Physical Sciences Research Council for funding this research through grant #EP/K033476/1. We are also grateful to Max Spencer and Jeunese Payne for useful discussions, and to Ben Wong for scheduling and running participants. The authors also thank Graham Johnson for assistance in reaching out to professional designers.

#### REFERENCES

- [1] D. Allouche, S. de Givry, and T. Schiex, "Toulbar2, an open source exact cost function network solver," Technical report, INRIA, Tech. Rep., 2010.
- [2] C. M. Arrington and G. D. Logan, "Voluntary task switching: chasing the elusive homunculus," *Journal of Experimental Psychology: Learning, Memory, and Cognition*, vol. 31, no. 4, p. 683, 2005.
- [3] F. G. Ashby and W. T. Maddox, "Human category learning 2.0," *Annals of the New York Academy of Sciences*, vol. 1224, no. 1, pp. 147–161, 2011.
- [4] A. Baddeley, "Working memory: theories, models, and controversies," *Annual review of psychology*, vol. 63, pp. 1–29, 2012.
- [5] A. Beauteament, M. A. Sasse, and M. Wonham, "The compliance budget: managing security behaviour in organisations," in *Proceedings of the 2008 workshop on New security paradigms*. ACM, 2009, pp. 47–58.
- [6] G. E. Box and N. R. Draper, *Empirical model-building and response surfaces*. John Wiley & Sons, 1987.
- [7] D. Cohen, J. Crampton, A. Gagarin, G. Gutin, and M. Jones, "Iterative plan construction for the workflow satisfiability problem," *J. Artif. Intell. Res. (JAIR)*, vol. 51, pp. 555–577, 2014. [Online]. Available: <http://dx.doi.org/10.1613/jair.4435>
- [8] A. L. Comrey, "Factor-analytic methods of scale development in personality and clinical psychology," *Journal of consulting and clinical psychology*, vol. 56, no. 5, p. 754, 1988.
- [9] J. Crampton, "A reference monitor for workflow systems with constrained task execution," in *Proceedings of the tenth ACM symposium on Access control models and technologies*. ACM, 2005, pp. 38–47.
- [10] D. de Waard and B. Lewis-Evans, "Self-report scales alone cannot capture mental workload," *Cognition, Technology & Work*, vol. 16, no. 3, pp. 303–305, 2014.
- [11] J. De Winter, "Controversy in human factors constructs and the explosive use of the nasa-tlx: a measurement perspective," *Cognition, technology & work*, vol. 16, no. 3, pp. 289–297, 2014.
- [12] P. E. Downing, "Interactions between visual working memory and selective attention," *Psychological Science*, vol. 11, no. 6, pp. 467–473, 2000.
- [13] C. J. Ferguson, "An effect size primer: A guide for clinicians and researchers," *Professional Psychology: Research and Practice*, vol. 40, no. 5, p. 532, 2009.
- [14] M. Gade and I. Koch, "The influence of overlapping response sets on task inhibition," *Memory & Cognition*, vol. 35, no. 4, pp. 603–609, 2007.
- [15] E. Hebrard, E. O'Mahony, and B. O'Sullivan, "Constraint Programming and Combinatorial Optimisation in Numberjack," in *Proceedings of the 7th International Conference on Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimization Problems (CPAIOR-10)*, ser. Lecture Notes in Computer Science, A. Lodi, M. Milano, and P. Toth, Eds., vol. 6140. Bologna, Italy: Springer-Verlag, May 2010, pp. 181–185.
- [16] P. G. Inglesant and M. A. Sasse, "The true cost of unusable password policies: password use in the wild," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2010, pp. 383–392.
- [17] B. E. John and D. E. Kieras, "The goms family of analysis techniques: Tools for design and evaluation," Tech. Rep., 1994.
- [18] B. E. John, E. W. Patton, W. D. Gray, and D. F. Morrison, "Tools for predicting the duration and variability of skilled performance without skilled performers," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 56, no. 1. SAGE Publications, 2012, pp. 985–989.
- [19] D. S. Johnson, "The np-completeness column: An ongoing guide," *Journal of Algorithms*, vol. 3, no. 2, pp. 182–195, 1982.
- [20] A. Kiesel, M. Steinhauser, M. Wendt, M. Falkenstein, K. Jost, A. M. Philipp, and I. Koch, "Control and interference in task switching: a review," *Psychological bulletin*, vol. 136, no. 5, p. 849, 2010.
- [21] V. Kumar, "Algorithms for constraint-satisfaction problems: A survey," *AI magazine*, vol. 13, no. 1, p. 32, 1992.
- [22] J. S. Rubinstein, D. E. Meyer, and J. E. Evans, "Executive control of cognitive processes in task switching," *Journal of Experimental Psychology: Human Perception and Performance*, vol. 27, no. 4, p. 763, 2001.
- [23] R. Sandhu and B. J. Dyson, "Modality and task switching interactions using bi-modal and bivalent stimuli," *Brain and cognition*, vol. 82, no. 1, pp. 90–99, 2013.
- [24] M. A. Sasse, M. Steves, K. Krol, and D. Chisnell, "The great authentication fatigue—and how to overcome it," in *Cross-Cultural Design*. Springer, 2014, pp. 228–239.
- [25] T. Schiex, H. Fargier, G. Verfaillie *et al.*, "Valued constraint satisfaction problems: Hard and easy problems," *IJCAI (1)*, vol. 95, pp. 631–639, 1995.
- [26] R. Shay, S. Komanduri, A. L. Durity, P. S. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, and L. F. Cranor, "Can long passwords be secure and usable?" in *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2014, pp. 2927–2936.
- [27] M. Steves, D. Chisnell, A. Sasse, K. Krol, M. Theofanos, and H. Wald, "Report: Authentication diary study," 2014.
- [28] T. Strobach, R. Liepelt, T. Schubert, and A. Kiesel, "Task switching: effects of practice on switch and mixing costs," *Psychological Research*, vol. 76, no. 1, pp. 74–83, 2012.
- [29] N. Yeung and S. Monsell, "Switching between tasks of unequal familiarity: the role of stimulus-attribute and response-set selection," *Journal of Experimental Psychology: Human Perception and Performance*, vol. 29, no. 2, p. 455, 2003.
- [30] Y. Zhang, R. Padman, and J. E. Levin, "Reducing provider cognitive workload in cpoe use: optimizing order sets," *Studies in health technology and informatics*, vol. 192, pp. 734–738, 2012.



# Stealing PINs via Mobile Sensors: Actual Risk versus User Perception

Maryam Mehrnezhad, Ehsan Toreini, Siamak F. Shahandashti, Feng Hao  
School of Computing Science, Newcastle University, UK  
Email: {m.mehrnezhad, ehsan.toreini, siamak.shahandashti, feng.hao}@ncl.ac.uk

**Abstract**—In the first part of this paper, we propose PINlogger.js which is a JavaScript-based side channel attack revealing user PINs on an Android mobile phone. In this attack, once the user visits a website controlled by an attacker, the JavaScript code embedded in the web page starts listening to the motion and orientation sensor streams without needing any permission from the user. By analysing these streams, it infers the user’s PIN using an artificial neural network. Based on a test set of fifty 4-digit PINs, PINlogger.js is able to correctly identify PINs in the first attempt with a success rate of 82.96%, which increases to 96.23% and 99.48% in the second and third attempts respectively. The high success rates of stealing user PINs on mobile devices via JavaScript indicate a serious threat to user security.

In the second part of the paper, we study users’ perception of the risks associated with mobile phone sensors. We design user studies to measure the general familiarity with different sensors and their functionality, and to investigate how concerned users are about their PIN being discovered by an app that has access to all these sensors. Our results show that there is significant disparity between the actual and perceived levels of threat with regard to the compromise of the user PIN. We discuss how this observation, along with other factors, renders many academic and industry solutions ineffective in preventing such side channel attacks.

## I. INTRODUCTION

Smartphones equipped with many different sensors such as *GPS*, *light*, *orientation* and *motion* are continuously providing more features to end users in order to interact with their real-world surroundings. Developers can have access to the mobile sensors either by 1) writing native code using mobile OS APIs [16], 2) recompiling HTML5 code into a native app [32], or 3) using standard APIs provided by the W3C which are accessible through JavaScript code within a mobile browser<sup>1</sup>. The last method has the advantage of not needing any app-store approval for releasing the app or doing future updates. More importantly, the JavaScript code is platform independent,

<sup>1</sup>[w3.org/TR/#tr\\_Javascript\\_APIs](http://w3.org/TR/#tr_Javascript_APIs)

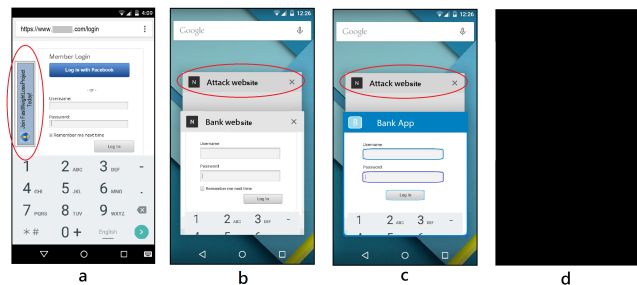


Fig. 1. PINlogger.js potential attack scenarios; a) the malicious code is loaded in an iframe and the user is on the same tab, b) the attack tab is already open and the user is on a different tab, c) the attack content is already open in an installed app, and the user is on an installed app, d) the attack content is already open in a (minimised) browser, and the screen is locked. The attacker listens to the side channel motion and orientation measurements of the victim’s mobile device through JavaScript code, and uses machine learning methods to discover the user’s sensitive information such as activity types and PINs.

i.e., once the code is developed it can be executed within any modern browser on any mobile OS.

**In-browser access risks.** While sensor-enabled mobile web applications provide users more functionalities, they raise new privacy and security concerns. Both the academic community and the industry have recognised such issues regarding certain sensors such as geolocation [18]. For a website to access the geolocation data, it must ask for explicit user permission. However, to the best of our knowledge, there is little work evaluating the risks of in-browser access to other sensors. Unlike in-app attacks, an in-browser attack, i.e., via JavaScript code embedded in a web page, does not require any app installation. Furthermore, JavaScript code does not require any user permission to access sensor data such as device motion and orientation. Furthermore, there is no notification while JavaScript is reading the sensor data stream. Hence, such in-browser attacks can be carried out far more covertly than the in-app counterparts. However, an effective in-browser attack still has to overcome the technical challenge that the sampling rates available in browser are much lower than those in app. For example, as we observed in [22], frequency rates of motion and orientation sensor data available in-browser are 3 to 5 times lower than those of accelerometer and gyroscope available in-app.

**Motion and orientation sensors detail.** According to W3C specifications [1] motion and orientation sensor data are a series of different measurements:

- device *orientation* which provides the physical orientation of the device, expressed as three rotation angles ( $\alpha$ ,  $\beta$ ,  $\gamma$ ) in the device’s local coordinate frame,
- device *acceleration* which provides the physical acceleration of the device, expressed in Cartesian coordinates ( $x$ ,  $y$ ,  $z$ ) in the device’s local coordinate frame,
- device *acceleration-including-gravity* which is similar to acceleration except that it includes gravity as well
- device *rotation rate* which provides the rotation rate of the device about the local coordinate frame, expressed as three rotation angles ( $\alpha$ ,  $\beta$ ,  $\gamma$ ), and
- *interval* which provides the constant sampling rate and is expressed in milliseconds (ms).

The device coordinate frame is defined with respect to the standard position of the mobile screen. When it is in the portrait mode,  $x$  and  $y$  axes are in the plane of the screen and are positive towards the screen’s right and up, and  $z$  is perpendicular to the plane of the screen and is positive outwards from the screen. Moreover, the sensor data discussed above are processed sensor data obtained from multiple physical sensors such as gyroscope and accelerometer. In the rest of this paper, unless specified otherwise, by sensor data we mean the sensor data accessible through mobile browsers which includes acceleration, acceleration-including-gravity, rotation rate, and orientation.

**Motivation.** Many popular browsers such as Safari, Chrome, Firefox, Opera and Dolphin have already implemented access to the above sensor data. As we demonstrated in [21] and [22], all of these mobile browsers allow such access when the code is placed in any part of the active tab including *iframes* (Figure 1, a). In some cases such as Chrome and Dolphin on iOS, an inactive tab including the sensor listeners have access to the sensor measurements as well (Figure 1, b). Even worse, some browsers such as Safari allow the inactive tabs to access the sensor data, when the browser is minimised (Figure 1, c), or even when the screen is locked (Figure 1, d). Mobile operating systems and browsers do not seem to be implementing consistent access control policies in regard to mobile orientation and motion sensor data. Furthermore, W3C specifications [1] do not discuss any risks associated with this potential vulnerability. Because of the low sampling rates available in browser, the community have been neglecting the security risks associated with in-browser access to such sensor data. However, in TouchSignatures [22], we showed that despite the low sampling rates, it is possible to identify user touch actions such as click, scroll, and zoom and even the numpad’s digits. In this work we contribute to the study of such attacks as follows:

- We introduce PINLogger.js, an attack on full 4-digit PINs as opposed to only single digits in [22]. We show that unregulated access to these sensors impose more serious security risks to the users in comparison with more well-known sensors such as camera, light and microphone.
- We conduct user studies to investigate users’ understanding about these sensors and also their perception of the

security risks associated with them. We show that users in fact have fewer security concerns about these sensors comparing to more well-known ones.

- We study and challenge current suggested solutions, and discuss why our studies show they cannot be effective. We argue that a usable and secure solution is not straightforward and requires further research.

## II. PINLOGGER.JS

In this section, we describe an advanced attack on user’s PINs by introducing PINlogger.js. In the following subsections, we describe the attack approach, our program implementation, data collection, feature extraction, and neural network.

### A. Attack approach

We consider an attacker who wants to learn the user’s PIN tapped on a soft keyboard of a smartphone via side channel information. We consider (digit-only) PINs since they are popular passwords used by users for many purposes such as unlocking phone, SIM PIN, NFC payments, bank cards, other banking services, gaming, and other personalised applications such as healthcare, insurance, etc. Unlike similar works which have to gain the access through an installed app [23], [27], [24], [10], [29], [30], [26], [33], [3], [11], our attack does not require any user permission. Instead, we assume that the user has loaded the malicious web content in the form of an *iframe*, or another tab while working with the mobile browser as shown in Figure 1. At this point, the attack code has already started listening to the sensor sequences from the user’s interaction with the phone.

In order to uncover when the user enters his PIN, we need to classify his touch actions such as click, scroll, and zoom. We already have shown in TouchSignatures [22] that with the same sensor data and by applying classification algorithms, it is possible to effectively identify user’s touch actions. Here, we consider a scenario after the touch action classification. In other words, our attacker already knows that the user is entering his PIN. Moreover, unless explicitly noted, we consider a generic attack scenario which is not user-dependant. This means that we do not need to train our machine learning algorithm with the same user as the subject of the attack. Instead, we have a one-round training phase with data from multiple voluntary users, and use the obtained trained algorithm to output other users’ PINs later. This approach has the benefit of not needing to trick individual users to collect data for training.

### B. Web program implementation

We implemented a web page with embedded JavaScript code in order to collect the data from voluntary users. Our code registers two listeners on the window object to have access to orientation and motion data, separately. The event handlers defined for these purposes are named *DeviceOrientationEvent* and *DeviceMotionEvent*, respectively. On the client side, we developed a GUI in HTML5 which shows random 4-digit PINs to the users and activates a numpad for them to enter the



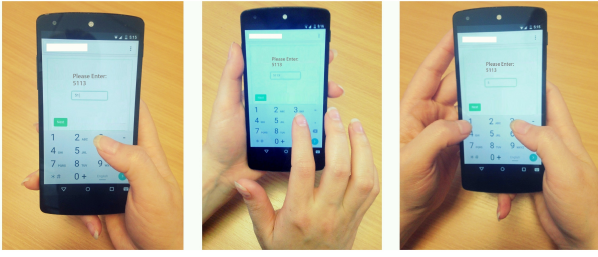


Fig. 2. Different input methods used by the users for PIN entrance.

PINs as shown in Figure 2. All sensor sequences are sent to the database along with their associated labels which are the digits of the entered PINs. We implemented our server program using Node.js (nodejs.org). Our code sends the orientation and motion sensor data of the mobile device to our NoSQL database using MongoLab (mongolab.com, web-based service for MongoDB). When the event listener fires, it establishes a socket by using Socket.IO (socket.io) between the client and the server and constantly transmits the sensor data to the database. Both Node.js and MongoDB (as a document-oriented database) are known for being capable of supporting data intensive applications in real time.

### C. Data collection

Following the approach of Aviv et al. [3] and Spreitzer [30], we consider a set of 50 fixed random PINs in this paper. We conducted our user studies using Chrome on an Android device (Nexus 5). The experiments and results are based on the collected data from 5 users, each entering all the 50 4-digit PINs for 5 times. Our voluntary participants were university students and staff and performed the experiments at university offices. We simply explained to them that all they needed was to enter a few PINs shown in a web page.

In relation to the environmental setting for the data collection, we asked the users to remain sitting in a chair while working with the phone. We did not require our users to hold the phone in any particular mode (portrait or landscape) or work with it by using any specific input method (using one or two hands). We let them choose their most comfortable posture for holding the phone and working with it as they do in their usual manner. While watching the users during the experiments, we noticed that all of our users used the phone in the portrait mode by default. Users were either leaning their hands on the desk or freely keeping them in the air. We also observed the following input methods used by the users.

- Holding the phone in one hand and entering the PIN with the thumb of the same hand (Figure 2, left).
- Holding the phone in one hand and entering the PIN with the fingers of the other hand (Figure 2, centre).
- Holding the phone with two hands and entering the PIN with the thumbs of both hands (Figure 2, right).

In the first two cases, users exchangeably used either their right hands or left hands in order to hold the phone. In order to simulate a real world data collection environment, we took

the phone to each user’s workspace and briefly explained the experiment to them, and let them complete the experiment without our supervision. All users found this way of data collection very easy and could finish the experiments without any difficulties.

### D. Feature extraction

In order to build the feature vector as the input to our classifier algorithm, we consider both time domain and frequency domain features. We improve our suggested feature vectors in [22] by adding some more complex features such as the correlation between the measurements. This addition improves the results, as we will discuss in Section III. As discussed before, 12 different sequences obtained from the collected data include orientation (ori), acceleration (acc), acceleration-including-gravity (accG), and rotation rate (rotR) with three sequences (either  $x$ ,  $y$  and  $z$ , or  $\alpha$ ,  $\beta$  and  $\gamma$ ) for each sensor measurement. As a pre-processing step and in order to remove the effect of the initial position and orientation of the device, we subtract the initial value in each sequence from subsequent values in the sequence.

We use these pre-processed sequences for feature extraction in time domain directly. In frequency domain, we apply the Fast Fourier transform (FFT) on the pre-processed sequences and use the transformed sequences for feature extraction. In order to build our feature vector, first we obtain the maximum, minimum, and average values of each pre-processed and FFT sequences. These statistical measurements give us  $3 \times 12 = 36$  features in the time domain, and the same number of features in the frequency domain. We also consider the total energy of each sequence in both time and frequency domains calculated as the sum of the squared sequence values, i.e.,  $E = \sum v_i^2$  which gives us 24 new features.

The next set of features are in time domain and are based on the correlation between each pair of sequences in different axes. We have 4 different sequences; ori, acc, accG, and rotR, each represented by 3 measurements. Hence, we can calculate 6 different correlation values between the possible pairs; (ori, acc), (ori, accG), (ori, rotR), (acc, accG), (acc, rotR), and (accG, rotR), each presented in a vector with 3 elements. We use the Correlation coefficient function in order to calculate the similarity rate between the mentioned sequences. The correlation coefficient method is commonly used to compare the similarity of the shapes of two signals (e.g. [5]). Given two sequences  $A$  and  $B$  and  $Cov(A, B)$  denoting covariance between  $A$  and  $B$ , the correlation coefficient is computed as below:

$$R_{AB} = \frac{Cov(A, B)}{\sqrt{Cov(A, A) \cdot Cov(B, B)}} \quad (1)$$

The correlation coefficient of two vectors measures their linear dependence by using covariance. By adding these new 18 features, our feature vector consists of a total of 114 features.

Attempts	Identification rate
One	82.96%
Two	96.23%
Three	99.48%

TABLE I

PINLOGGER.JS'S PIN IDENTIFICATION RATES IN DIFFERENT ATTEMPTS.

Attempts	User independent	User dependent
One	71.57%	80.21%
Two	82.83%	90.24%
Three	92.01%	95.05%

TABLE II

AVERAGE DIGIT IDENTIFICATION RATES IN DIFFERENT ATTEMPTS.

### E. Neural network

We apply a supervised machine learning algorithm by using an Artificial Neural Network (ANN) to solve this classification problem. The input of an ANN system could be either raw data, or pre-processed data from the samples. In our case, we have preprocessed our samples by building a feature vector as described before. Therefore, as input, our ANN receives a set of 114 features for each sample. As explained before, we collected 5 sample per each 4-digit PINs from 5 different users, giving us 1250 feature vectors in general.

The feature vectors are mapped to specific labels from a finite set: i.e., 50 fixed random 4-digit PINs. We train and validate our algorithm with two different subsets of our collected data, and test the neural network against a separate subset of the data. We train the network with 70% of our data, validate it with 15% of the records and test it with the remaining 15% of our data set. We use a pattern recognition/classifying network in Matlab with one hidden layer and 1000 nodes. Pattern recognition/classifying networks normally use a scaled conjugate gradient (SCG) back-propagation algorithm for updating weight and bias values in training. Scaled conjugate gradient is a fast supervised learning algorithm [25].

## III. EVALUATION

In this section we present the results of our attack and compare them with other works.

### A. PINlogger.js success rate

Table I shows the accuracy of our ANN trained with the data from all users. Since these results are based on the collected data from all users, we refer to it as the user-independent mode. As the table shows, in the first attempt PINlogger.js is able to infer the user's 4-digit PIN correctly with accuracy of 82.96%. The results get better on further attempts. As the table shows, our system is able to reveal the user's PIN with nearly 100% accuracy in three attempts. By comparison, a random attack can guess a PIN from a set of 50 PINs with the probability of 2% in the first attempt, and 6% in three attempts.

### B. User-dependent mode

In order to study the impact of individual training, we trained, validated and tested the network with the data collected from one user. We refer to this mode of analysis as the user-dependent mode. We asked our user to enter 50 random PINs, each five times, and repeat the experiment for 5 times (rounds). The reason we have repeated the experiments is that the classifier needs to receive enough samples to be able to train the system. Interestingly, our user used all three different

input methods shown in Figure 2 during the PIN entrance. As expected, our classifier performs better when it is personalized: the accuracy increases to 91.42% in the first attempt, and 98.64% and 100% in two and three attempts, respectively.

In the user-dependent mode, convincing the users to provide the attacker with sufficient data for training customised classifiers is not easy, but still possible. Approaches similar to gaming apps such as Math Trainer<sup>2</sup> could be applied. Math-based CAPTCHAs are possible web-based alternatives. Any other web-based game application which segments the GUI similar to a numerical keypad will do as well. Nonetheless, this is out of the scope of this paper since we mainly follow a user-independent approach.

### C. Guessing the PIN from the entire PIN space

One might argue that the attack should be evaluated against the whole 4-digit PIN space. However, we believe that the attack could still be practical when selecting from a limited set of PINs since users do not select their PINs randomly [8]. It has been reported that around 27% of all possible 4-digit PINs belong to a set of 20 PINs<sup>3</sup>, including straightforward ones like '1111', '1234', or '2000'. Nevertheless, we present the results of our analysis of the attack against the entire search space for both the user-independent and user-dependent modes.

For user-independent mode, we trained another ANN in order to infer a single digit on the numpad. In this experiment, we considered 10 classes of the entered digits (0–9) from the data we collected on 4-digit PINs used in Section III-A. For user-dependent mode, we trained personalised classifiers for each user. Unlike the test condition of Section III-B, we did not have to increase the number of rounds of PIN entry here since we had enough samples for each digit per user. Hence in the user-dependent mode in this section, we used the average of the results of our 5 users. The average identification rates of different digits are presented in Table II.

The results in our user-independent mode show that it is possible to correctly infer digits in over 71% of the cases in the first attempt, going up to 92% in three attempts. This means that for a 4-digit PIN and based on the obtained sensor data, the attacker can guess the PIN to be within a set of  $3^4 = 81$  possible PINs with a probability of success equal to  $0.92^4 = 71.67\%$ . A random attack, however, can only predict the 4-digit PIN with the probability of 0.81% in 81 attempts. By comparison, PINlogger.js achieves a dramatically higher success rate than a random attacker. Using a similar argument, in the user-dependent mode the success probability of guessing the PIN in 81 attempts is 81.62%. In the same setting, Cai and

<sup>2</sup>play.google.com/store/apps/details?id=com.solirify.mathgame

<sup>3</sup>datagenetics.com/blog/september32012/

Featured Work	PIN Skimming [30]	PIN Skimmer [29]	Keylogging by Mic [26]	TapLogger [33]	Acc. side channel [3]	PINlogger.js	
Sensor Access type	Light in-app	Camera, Mic in-app	Mic, Gyr in-app	Acc, Ori in-app	Acc in-app	Motion, Ori in-browser	
Training approach	user-dependent	user-dependent	user-dependent	user-dependent	user-independent	user-independent	user-dependent
Identification rate							
First attempt	NA	NA	94%	40%	18%	82.96%	91.42%
Second attempt	50%	30%	NA	75%	NA	96.23%	98.64%
Fifth attempt	65%	50%	NA	100%	43%	100%	100%

TABLE III  
COMPARISON OF PINLOGGER.JS WITH RELATED ATTACKS ON 4-DIGIT PINs.

Chen report a success rate of 65% using accelerometer and gyroscope data [2] and Simon and Anderson’s PIN Skimmer only achieves a 12% success rate in 81 attempts using camera and microphone [29]. Our results in digit recognition in this paper are also better than what is achieved in TouchSignatures [22]. In summary, PINlogger.js performs better than all sensor-based digit-identifier attacks in the literature.

#### D. Comparison with related work

Obtaining sensitive information about users such as PINs based on mobile sensors through a malicious app running in the background has been actively explored by researchers in the field. For example, GyroPhone, by Michalevsky et al. [23], shows that gyroscope data is sufficient to identify the speaker and even parse speech to some extent. Other examples include Accessory [27] by Owusu et al. and Tappprints [24] by Miluzzo. They infer passwords on full alphabetical soft keyboards based on accelerometer measurements. Touchlogger [10] is another example by Cai and Chen [2] which shows the possibility of distinguishing user’s input on a mobile numpad by using accelerometer and gyroscope. The same authors demonstrate a similar attack in [11] on both numerical and full keyboards. The only work which relies on in-browser access to sensors to attack a numpad is our previous work, TouchSignatures [22]. All of these works, however, aim for the individual digits or characters of a keyboard, rather than the entire PIN or password.

Another category of works directly target user PINs. For example, PIN skimmer by Simon and Anderson [29] is an attack on a user’s numpad and PINs using the camera and microphone on the smartphone. Spreitzer suggests another PIN Skimming attack [30] and steals a user’s PIN based on the measurements from the smartphone’s ambient light sensor. Narain et al. introduce another attack [26] on smartphone numerical and alphabetical keyboards and the user’s PINs and credit card numbers by using the smartphone microphone. TapLogger by Xu et al. [33] is another attack on the smartphone numpad which outputs the pressed digits and PINs based on accelerometer and orientation sensor data. Similarly, Aviv et al. introduce an accelerometer-based side channel attack on the user’s PINs and patterns in [3]. We choose to compare PINlogger.js with the works in this category since they have the same goal of revealing the user’s PINs. Table III presents the results of our comparison.

As shown in Table III, PINlogger.js is the only attack on PINs which acquires the sensor data via JavaScript code. In-browser JavaScript-based attacks impose even more security threats to users since unlike in-app attacks, they do not require any app installation and user permission to work. Moreover, the attacker does not need to develop different apps for different platforms such as Android, iOS, and Windows. Once the attacker develops the JavaScript code, it can be deployed to attack all mobile devices regardless of the platform. Moreover, Touchlogger.js and [3] are the only user-independent works. By contrast, the results form other works are based on training the classifiers for individual users. In other words, they assume the attacker is able to collect input training data from the victim user before launching the PIN attack. We do not have such an assumption as the training data is obtained from all users in the experiment. In terms of accuracy, with the exception of [26], PINlogger.js generally outperforms other works with an identification rate of 82.96% in the first try, and 96.23% and 100% in the second and fifth attempts, respectively. This is a significant success rate (despite that the sampling rate in-browser is much lower than that available in-app) and confirms that the described attack imposes a serious threat to the users’ security and privacy.

#### IV. WHY DOES THIS VULNERABILITY EXIST?

Although reports of side channel attacks based on the in-browser access to mobile sensors via JavaScript are relatively recent, similar attacks via in-app access to mobile sensors have been known for years. Yet the problem has not been fixed.

We believe a contributing factor is that users seem to be less familiar with the relatively newer (and less advertised) sensors such as motion and orientation, as opposed to their immediate familiarity with well-established sensors such as camera and GPS. For example, a user has asked this question on a mobile forum: “... What benefits do having a gyroscope, accelerometer, proximity sensor, digital compass, and barometer offer the user? I understand it has to do with the phone orientation but am unclear in their benefits. Any explanation would be great! Thanks!”<sup>4</sup>.

We design and conduct user studies in this work in order to investigate to what extent are these sensors and their risks known to the users.

<sup>4</sup>forums.androidcentral.com/verizon-galaxy-nexus/171482-barometer-accelerometer-how-they-useful.html

### A. List of mobile sensors

We prepared a list of different mobile sensors by inspecting the official websites of the latest iOS and Android products, and the specifications that W3C and Android provide for developers. We also added some extra sensors as common sensing mobile hardware which are not covered before.

- iPhone 6<sup>5</sup>: Touch ID, Barometer, Three-axis gyro, Accelerometer, Proximity sensor, Ambient light sensor.
- Nexus 6P<sup>6</sup>: Fingerprint sensor, Accelerometer, Gyroscope, Barometer, Proximity sensor, Ambient light sensor, Hall sensor, Android Sensor hub.
- Android [16]: Accelerometer, Ambient temperature, Gravity (software or hardware), Gyroscope, Light, Linear Acceleration (software or hardware), Magnetic Field, Orientation (software), Pressure, proximity, Relative humidity, Rotation vector (Software or Hardware), Temperature.
- W3C<sup>7</sup> [1]: Device orientation (software), Device motion (software), Ambient light, Proximity, Ambient temperature, Humidity, Atmospheric Pressure.
- Extra sensors (Common sensing hardware): Wireless technologies (WiFi, Bluetooth, NFC), Camera, Microphone, Touch screen, GPS.

Unless specified otherwise, all the listed sensors are hardware sensors. We added the last category of the sensors to this list since they indeed sense the device’s surrounding although in different ways. However, they are neither counted as sensors in mobile product descriptions, nor in technical specifications. These sensors are often categorised as OS resources [31], and hence different security policies apply to them.

### B. User study

We prepared a list of sensors based on the above. We asked volunteer participants to rate the level of their familiarity with each sensor. In all of our studies, we had 30 participants (13 self-identified as male and 17 as female) recruited from the university and local community through social and vocational networks, from 18 to 59 years old, with a median age of 31. Except one, none of the participants were studying or working in the field of computer security. Our university participants were from multiple degree programs and levels, and the remaining participants worked in a different range of fields. Moreover, our participants owned a wide range of mobile devices, and had been using a smartphone/tablet for 6 years on average (from 0 to 11 years). We interviewed our participants at a university office and gave each an Amazon voucher (worth £10) at the end for their participation. Details of the interview template can be found in the Appendix.

For a list of 25 different sensors, we used a five-point scale self-rated familiarity questionnaire as used in [19]: “I’ve never heard of this”, “I’ve heard of this, but I don’t know what this is”, “I know what this is, but I don’t know how this works”, “I know generally how this works”, and “I know very well how

this works”. The list of sensors was randomly ordered for each user to minimize bias. In addition, we needed to observe the experiments to make sure users were answering the questions based on their own knowledge in order to avoid the effect of processed answers. Full descriptions of all studies are provided in the Appendix. Fig. 3 summarizes the results of this study.

Our participants were generally surprised to hear about some sensors and impressed by the variety. As one may expect, newer sensors tend to be less known to the users in comparison to older ones. In particular, our participants were generally not familiar with ambient sensors. Also low-level hardware sensors such as accelerometer and gyroscope, seem to be less known to the users in comparison with high-level software ones such as motion, orientation, and rotation. We suspect that this is partly due to the fact that the high-level sensors are named after their functionalities and can be more immediately related to user activities.

We also noticed that a few of the participants knew some of the low-level sensors by name but they could not link them to their functionality. For example, one of our participants which knew almost all of the listed sensors (except hall sensor and sensor hub) stated that: “When I want to buy a mobile [phone], I do a lot of search, that is why I have heard of all of these sensors. But, I know that I do not use them (like accelerometer and gyroscope)”.

On the other hand, as the functionalities of mobile devices grow, vendors quite naturally turn to promote the software capabilities of their products, instead of introducing the hardware. For example, many mobile devices are recognised for their gesture recognition features by the users, however the same users might not know how these devices provide such a feature. For instance, one of the participants commented on a feature on her smartphone called “Smart Stay”<sup>8</sup> as follows: “I have another sensor on my phone: Smart Stay. I know how it works, but I don’t know which sensors it uses”.

## V. RISK PERCEPTION OF MOBILE SENSORS

In this section, we study the participants’ risk perception of mobile sensors. There have been several studies on risk perception addressing different aspects of mobile technology. Some works discuss the risks that users perceive on smartphone authentication methods such as PINs and patterns [17], TouchID and Android face unlock [14], and implicit authentication [20]. Other works focus on the privacy risks of certain sensors such as GPS [4]. In [28], Raji et al. show users’ concerns (on disclosure of selected behaviours and contexts) about a specific sensor-enabled device called AutoSense<sup>9</sup>. To the best of our knowledge, the research presented in this paper is the first that studies the user risk perception for a comprehensive list of mobile sensors (25 in total). We limit our study to the level of perceived risks users associate with their PINs being discovered by each sensor. The reasons we chose PINs are that first, finding one’s PIN is a clear and

<sup>5</sup>apple.com/uk/iphone-6/specs/

<sup>6</sup>store.google.com/product/nexus\_6p

<sup>7</sup>w3.org/2009/dap/

<sup>8</sup>samsung.com/us/support/answer/ANS00035658/234302/SCH-R950TSAUSC

<sup>9</sup>sites.google.com/site/autosenseproject/

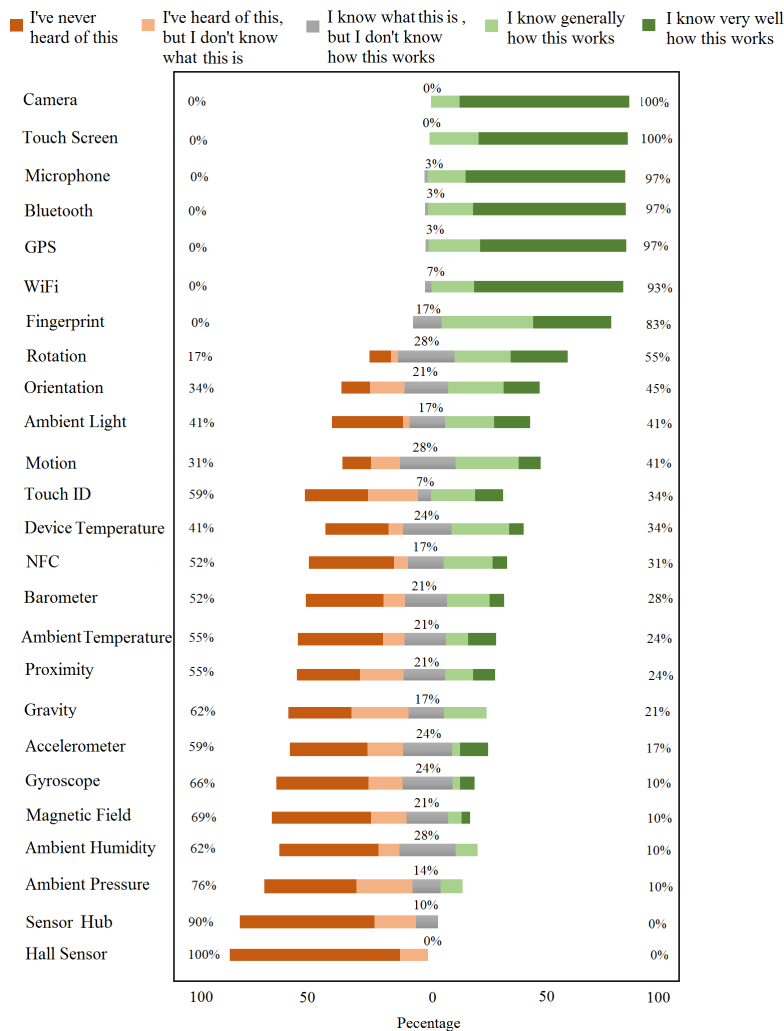


Fig. 3. Level of self-declared knowledge about different mobile sensors. Question: “To what extent do you know each sensor on a mobile device?” Sensors are ordered based on the aggregate percentage of participants declaring they know generally or very well how each sensor works. This aggregate percentage is shown on the right hand side.

intuitive security risk, and second, we can put the perceived risk levels in context with respect to the actual risk levels for a number of sensors as described in Table III.

#### A. Methodology

For this study, we interviewed the same group of users from Section IV-B in two phases. In phase one, we gave the same sensor list (randomized for each user). We asked users to rate the level of risk they perceive for each sensor in regards to revealing their PINs. We described a specific scenario in which a game app which has access to all these sensors is open in the background and the user is working on his online banking app, entering a PIN. We used a self-rated questionnaire with five-point scale answers following the same terminology as used in [28]: “Not concerned”, “A little concerned”, “Moderately concerned”, “Concerned”, and “Extremely concerned”. During this phase, we asked the users to rely on the information that they already had about each sensor (see the Appendix for details).

In the second phase, first we provided the participants with a short description of each sensor and let them know that they can ask further questions until they feel confident that they understand the functionality of all sensors. Afterwards, we asked the participants to fill in another copy of the same questionnaire on risk perceptions (details in the Appendix). The results are presented in Fig. 4.

#### B. Intuitive risk perception

We make the following observations from the results of the experiment.

**Touch Screen.** Although our participants rated touch screen as one of the most risky sensors in relation to a PIN discovery scenario, still about half of our participants were either moderately concerned, a little concerned, or not concerned at all. Through our conversations with the users, we received some interesting comments, e.g., “Why any of these sensors should be dangerous on an app while I have officially installed it from a legal place such as Google Play?”, and “As long as the app

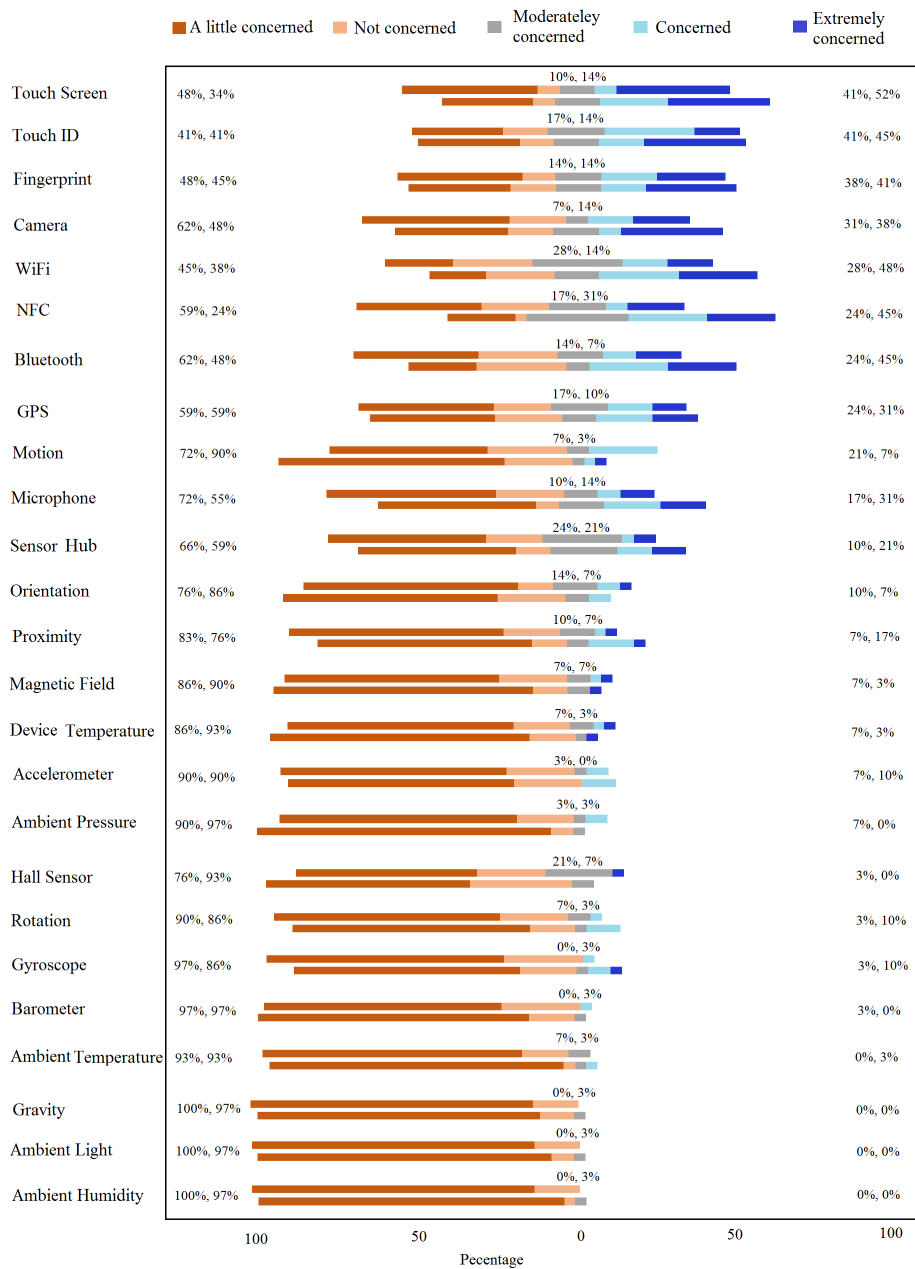


Fig. 4. Users' perceived risk for different mobile sensors, before (top bars) and after (bottom bars) being presented with descriptions of sensors. Question: "To what extent are you concerned about each sensor's risk to your PIN?". Sensors are ordered based on the aggregate percentage of participants declaring they are either concerned or extremely concerned about each sensor before seeing the descriptions. This aggregate percentage is the first value presented on the right hand side.

with these sensors is in the background, I have no concern at all". It seems that a more general risk model in relation to mobile devices is affecting the users' perception in regard to the presented PIN discovery threat. This fact can be a topic of research on its own, and is out of the scope of this paper.

**Communicational Sensors.** One category of the sensors which users are relatively more concerned about includes WiFi, Bluetooth and NFC. For example one of the participants commented that: "I am not concerned with physical

[motion, orientation, accelerometer, etc.]/ environmental [light, pressure, etc.] sensors, but network ones. Hackers might be able to transfer my information and PIN". This comment is understandable since we asked them to what extent they were concerned about *each sensor* in regard to the PIN discovery.

**Identity-related Sensors.** Another category which has been rated more risky than others contains those sensors which can capture something related to the user's identity i.e. fingerprint, TouchID, GPS, camera, and microphone. Despite that we

described a PIN-related scenario, our participants were still concerned about these sensors. This was also pointed out by a few participants through the comments. For example a user stated: “..., however, GPS might reveal the location along with the user input PIN that has a risk to reveal who (and where) that PIN belongs to. Also the fingerprint/TouchID might recognize and record the biometrics with the user’s PIN”. Some of these sensors such as GPS, fingerprint, and TouchID, however, can not cause the disclosure of PINs on their own. Hence, the concern does not entirely match the actual risk. Similar to the discussion on touch screen, we believe that a more general risk model on mobile technology influences the users to perceive risk on specific threats such as the one we presented to them.

**Environmental Sensors.** The level of concern on ambient sensors (humidity, light, pressure, and temperature) is generally low and stays low after the users are provided with the description of the sensors (see Fig. 4). In many cases, our users expressed that they were concerned about these sensors simply because they did not know them: “[now that I know these sensors,] I am quite certain that movement/environmental sensors would not affect the security of personal id/passwords etc.”. In fact, researchers have reported that it is possible to infer the user’s PIN using the ambient light sensor data [30], although, to our knowledge, exploits of other environmental sensors have not been reported in the literature.

**Movement Sensors.** On the sensors related to the movement and the position of the phone (accelerometer, gyroscope, motion, orientation, and rotation), the users display varying levels of the risk perceptions. In some cases they are slightly more concerned, but in others they are less concerned once they know the functionality. Some of our users stated that since they did not know these sensors, they were not concerned at all, but others were more concerned when they were faced with new sensors. Overall, knowing, or not knowing these sensors has not affected the perceived risk level significantly, and they were rated generally low in both cases.

**Motion and Orientation Sensors.** The sensors which we used in our attack, namely orientation, rotation, and motion, have not been generally scored high for their risk in revealing PINs. Users do not seem to be able to relate the risk of these sensors to the disclosure of their PINs, despite that they seem to have an average general understanding about how they work. On hardware sensors such as accelerometer and gyroscope, the risk perception seems to be even lower. A few comments include: “In my everyday life, I don’t even think about these [movement] sensors and their security. There is nothing on the news about their risk”, and “I have never been thinking about these [movement] sensors and I have not heard about their risk”. On the other hand, some of the participants expressed more concerns for sensors that they were familiar with, as one wrote, “You always hear about privacy stuff for example on Facebook when you put your location or pictures”. Similarly, it seems that having a previous risk model is a factor that might explain the correlation between the user’s knowledge and their perceived risk.

### C. General knowledge versus risk perception

Figs. 3 and 4 suggest that there may be a correlation between the relative level of knowledge users have about sensors and the relative level of risk they perceive from them. We limit our attention to users’ knowledge before being presented with sensor descriptions. We confirm our observation of correlation using Spearman’s rank-order correlation measure.

Spearman’s correlation between the comparative knowledge (median: “I know what this is, but I don’t know how this works”, IQR: “I’ve never heard of this” – “I know very well how this works”) and the perceived risk about different sensors (median: “Not concerned”, IQR: “Not concerned” – “A little concerned”) was  $r = 0.61$  ( $p < 0.05$ ). This result supports that the more the users know about these sensors, the more concern they express about the risk of the sensors revealing PINs. We acknowledge that other methods of ranking the results, e.g. using median, produce slightly different final rankings. However, given the high confidence level of the above test, we expect the correlation to be supported if other methods of ranking are used.

Assuming that customer demand drives better security designs, the above correlation may explain why sensors that are newer to the market have not been considered as OS resources and consequently have not been subject to similar strict access control policies.

### D. Perceived risk vs the actual risk

We are specifically interested in the users’ relative risk perception of sensors in revealing their PINs in comparison to the actual relative risk level of these sensors. We list the results reported in the literature in Table III for the following sensors: light, camera, microphone, gyroscope, motion, and orientation. Fig. 4 shows that users generally have expressed more concern about sensors such as camera and microphone than accelerometer, gyroscope, orientation, and motion. This does not match the actual risk levels since the latter sensors allow PIN recovery with higher accuracy as we have shown in Section III. When asked after filling the questionnaire, most participants could not come up with realistic attack scenarios using camera and microphone. For microphone, some users thought they might say the PIN out loud. For camera, a few of our participants thought face recognition might be used to recover the PIN, hence they rated camera’s risk to their PINs high. One user thought the camera might capture the reflection of the entered PIN in her glasses.

Among our participants, one mentioned but described doubt about motion, orientation, accelerometer, and gyroscope being able to record the shakes of the mobile phone while entering a PIN after they saw the sensor descriptions: “I feel those positional sensors might be able to reveal something about my activities, for example if I open my banking app or enter my PIN. But it is extremely hard for different users, and when working with different hands and positions”. This participant expressed only “a little concern” about them, stating that: “..., and by little concern, I mean extremely little concern”. One of our participants was completely familiar with these



attacks and in fact had read some related papers. This user was “extremely concerned”. Other users who rated these sensors risky in general, said they were generally concerned about different sensors. One commented: “I can not think of any particular situation in which these sensors can steal my PIN, but the hackers can do everything these days.”

## VI. POSSIBLE SOLUTIONS

In this section, we discuss the current academic and industrial countermeasures to mitigate sensor-based attacks.

### A. Academic approach

Different solutions to address the in-app access attacks have been suggested in the literature: e.g., restricting the sensor to one app, reducing the sampling rate, temporal pause of the sensor on sensitive entries such as keyboard, rearranging keyboard for password entrance, asking for explicit permission from the user, ranking apps based on their similarities to malware, and obfuscating anomalies in sensor data [26], [3], [30], [33], [29], [23], [24], [27], [13], [6]. However, after many years of research on showing the serious security risks of sensors such as accelerometer and gyroscope, none of the major mobile platforms have revised their in-app access policy.

We believe that the risks of unmanaged sensors on mobile phones, specially through JavaScript code, are not known very well yet. More specifically, many OS/app level solutions such as asking for permissions at the installation time, or malware detection approaches would not work in the context of a web attack. In our previous work [22], we suggested to apply the same security policies as those for camera, microphone, and GPS for the motion and orientation sensors. Our suggestion was to set a multi-layer access control system on the OS and browser levels. However, the usability and effectiveness of this solution are arguable. First, asking too many permissions from the user for different sensors might not be usable. Furthermore, for some basic use cases such as gesture recognition to clear a web form, or adjusting the screen from portrait to landscape, it might not make sense to ask for user permission for every website. Second, with the increase of the number of sensors accessible through mobile browsers, this approach might not be effective due to the classic problem of sidestepping the security procedure by users when it is too much of a burden [9]. As stated by one of our participants: “I don’t mind these sensors being risky anyway. I don’t even review the permission list. I have no other choice to be able to use the app”. Moreover, as we have shown in Section IV, users generally do not understand the implications of these sensors on discovering their PINs for example, even though they know how these sensors work. Hence, such an approach might not be effective in practice.

### B. Industrial approach

**W3C Device Orientation Event Specification.** There is no Security and Privacy section in the latest official W3C Working Draft Document on Device Orientation Event [1]. However, at the time of writing this paper, a new version of the W3C

specification is being drafted, which includes a new section on security and privacy issues related to mobile sensors<sup>10</sup>, as suggested by us in [22]. The authors working on the revision of the W3C specification point out the problem of fingerprinting mobile devices [7], and touch action recovery [22] through these sensors, and suggest the following mitigations:

- “Do not fire events when the page where they were registered on is not visible or has been backgrounded.”
- “Fire events only on the top-level browsing context or same-origin nested iframes.”
- “Limit the frequency of events (typically 60 Hz seems to be sufficient).”

We believe that these measures may be too restrictive in blocking useful functionalities. For example, imagine a user consciously running a web program in the browser to monitor his daily physical activities such as walking and running. This program needs to continue to have access to the motion and orientation sensor data when the user is working on another tab or minimizes the browser. One might argue that such a program should be available as an app instead, hence the use case is not valid. However, it is expected that the boundary between installed apps and embedded JavaScript programs in the browser will gradually diminish [12].

**Mobile browsers.** As we showed in [22], browsers and mobile operating systems behave differently on providing access to sensors. Some allow access only on the active webpage and any embedded iframes (although with different origins), some allow access to other tabs, when browser is minimized, or even when the phone is locked. Hence, there is not a consistent approach across all browsers and mobile platforms. Reducing the frequency rate has been applied to all well-known browsers at the moment [22]. For instance, Chrome reduced the sensor readings from 200 Hz to 60 Hz due to security concerns<sup>11</sup>. However, our attack shows that security risks are still present even at lower frequencies. iOS and Android limit the maximum frequency rate of some sensors such as Gyroscope to 100 Hz and 200 Hz, respectively. It is expected that these frequencies will increase on mobile OSs in the near future and in-browser access is no exception. In fact, current mobile gyroscopes support much higher sampling frequencies, e.g., up to 800 Hz by STMicroelectronics (on Apple products), and up to 8000 Hz by InvenSense (on the Google Nexus range) [23]. With higher frequencies available, attacks such as ours can perform better in the future if adequate security countermeasures are not applied.

Following our report of the issue to Mozilla, starting from version 46 (released in April 2016), Firefox restricts JavaScript access to motion and orientation sensors to only top-level documents and same-origin iframes<sup>12</sup>. In the latest Apple Security Updates for iOS 9.3 (released in March 2016), Safari took a similar countermeasure by “suspending the availability of this

<sup>10</sup>[w3c.github.io/deviceorientation/spec-source-orientation.html](http://w3c.github.io/deviceorientation/spec-source-orientation.html)

<sup>11</sup>[bugs.chromium.org/p/chromium/issues/detail?id=421691](https://bugs.chromium.org/p/chromium/issues/detail?id=421691)

<sup>12</sup>[mozilla.org/en-US/security/advisories/mfsa2016-43/](https://mozilla.org/en-US/security/advisories/mfsa2016-43/)

[motion and orientation] data when the web view is hidden”<sup>13</sup>. However, we believe the implemented countermeasures should only serve as a temporary fix rather than the ultimate solution. In particular, we are concerned that it has the drawback of prohibiting potentially useful web applications in the future. For example, a web page running a fitness program has a legitimate reason to access the motion sensors even when the web page view is hidden. However, this is no longer possible in the new versions of Firefox and Safari. Our concern is confirmed by members in the Google Chromium team<sup>14</sup>, who also believe that the issue remains unresolved.

## VII. FURTHER DISCUSSION AND LIMITATIONS OF OUR WORK

As mentioned earlier, many of the suggested academic solutions either have not been applied by the industry as a practical solution, or have failed. Given the results in our user studies, designing a practical solution for this problem does not seem to be straightforward. A combination of different approaches might help researchers devise a usable and secure solution. Having control on granting access *before* opening a website and *during* working with it, in combination with a smart notification feature on the browser would probably achieve a balance between security and usability. Users should also have control on reviewing, updating and deleting these data, if stored by the website or shared with a third party *afterwards*. Solutions such as Taintroid [15], a tracking app for monitoring sources of sensitive data on a mobile which has been applied for GPS in [4] could be helpful. After all, it seems that an extensive study is required toward designing a permission framework which is usable and secure at the same time. Such research is a very important usable security and privacy topic to be explored further in the future.

We consider this work a pilot study that explores user risk perception on a comprehensive list of mobile sensors. We envisage the following future work to address these limitations and expand this work:

- *More Participants*: We performed our user studies on a set of users who were recruited from a wide range of backgrounds. Yet the number of the participants is limited. A larger set of participants will improve the confidence in the results. With a large and diverse set of participants, we can also study the effect of demographic factors on perceived risk.
- *Other Risks*: We studied the perceived risk on PINs as a serious and immediate risk to users’ security. The study can be expanded by studying users’ risk perception on other issues such as attackers discovering phone call timing, physical activities, or shopping habits.
- *Other Types of Access*: When interviewing our participants, we presented them with a scenario involving a game app which is installed on their smartphone. This only covers the in-app access to sensors. However,

people might express different risk levels for other types of access, e.g., in-browser access. This needs further investigation.

- *Issues with Training Users*. We decided to provide our participants with a short description of each sensor’s functionality (details in the Appendix, part 3). Furthermore, the participants were given the chance to ask as many questions as they wanted to fully understand the functionality of each sensor. This might not be the most effective way to inform users about sensors since some descriptions might seem too technical (and hence not fully understandable) to some users. How to inform users in an effective way is a complex topic of research which can be explored in the future. Besides, we used the same set of participants to generally compare the level of perceived risk before and after seeing sensor descriptions. An alternative approach is to use a different set of participants, i.e., to follow a between-subjects approach instead of a within-subjects one, which would have less bias if carefully designed. However, in order to get meaningful results, the between-subjects approach would require recruiting a larger number of participants.

## VIII. CONCLUSION

In this paper, we introduced PINlogger.js, a web-based program which reveals users’ PINs by recording the mobile device’s orientation and motion sensor data through JavaScript code. We also showed that users do not generally perceive a high risk about such sensors being able to steal their PINs. We discussed the complexity of designing a usable and secure solution to prevent the proposed attacks. Access to mobile sensor data via JavaScript is limited to only a few sensors at the moment. This will probably expand in the future, considering for instance the ongoing development of JavaScript-based operating systems such as Firefox OS<sup>15</sup>. Hence, designing a general mechanism for secure and usable sensor data management remains a crucial open problem for future research.

## IX. ACKNOWLEDGEMENTS

We would like to thank Dr. Kovila Coopamootoo from Newcastle University for her constructive feedback on designing the user studies of this paper. We also would like to thank the voluntary participants who contributed to our data collection and user studies. All our experiments were approved by Newcastle University’s ethical committee. The last three authors are supported by ERC Starting Grant No. 306994.

## REFERENCES

- [1] W3C Working Draft Document on Device Orientation Event. <http://www.w3.org/TR/orientation-event/>.
- [2] On the best sensor for keystrokes inference attack on android. *Procedia Technology*, 11(0):989 – 995, 2013. 4th International Conference on Electrical Engineering and Informatics, 2013.

<sup>13</sup>[support.apple.com/en-gb/HT206166](http://support.apple.com/en-gb/HT206166)

<sup>14</sup>[bugs.chromium.org/p/chromium/issues/detail?id=523320](http://bugs.chromium.org/p/chromium/issues/detail?id=523320)

<sup>15</sup>[developer.mozilla.org/en/docs/Mozilla/Firefox\\_OS/Platform/Architecture](http://developer.mozilla.org/en/docs/Mozilla/Firefox_OS/Platform/Architecture)

- [3] A. J. Aviv, B. Sapp, M. Blaze, and J. M. Smith. Practicality of accelerometer side channels on smartphones. In *Proceedings of the 28th Annual Computer Security Applications Conference*, pages 41–50. ACM, 2012.
- [4] R. Balebako, J. Jung, W. Lu, L. F. Cranor, and C. Nguyen. “little brothers watching you:” raising awareness of data leaks on smartphones. In *Symposium on Usable Privacy and Security*. ACM Association for Computing Machinery, July 2013.
- [5] D. Bichler, G. Stromberg, M. Huemer, and M. Löw. Key generation based on acceleration data of shaking processes. In J. Krumm, G. Abowd, A. Seneviratne, and T. Strang, editors, *UbiComp 2007: Ubiquitous Computing*, volume 4717 of *Lecture Notes in Computer Science*, pages 304–317. Springer Berlin Heidelberg, 2007.
- [6] H. Bojinov, Y. Michalevsky, G. Nakibly, and D. Boneh. Mobile device identification via sensor fingerprinting. *CoRR*, abs/1408.1416, 2014.
- [7] H. Bojinov, Y. Michalevsky, G. Nakibly, and D. Boneh. Mobile device identification via sensor fingerprinting. *CoRR*, abs/1408.1416, 2014.
- [8] J. Bonneau, S. Preibusch, and R. Anderson. A birthday present every eleven wallets? the security of customer-chosen banking pins. In A. Keromytis, editor, *Financial Cryptography and Data Security*, volume 7397 of *Lecture Notes in Computer Science*, pages 25–40. Springer Berlin Heidelberg, 2012.
- [9] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. Schechter. Your attention please: Designing security-decision uis to make genuine risks harder to ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS ’13, pages 6:1–6:12, New York, NY, USA, 2013. ACM.
- [10] L. Cai and H. Chen. Touchlogger: Inferring keystrokes on touch screen from smartphone motion. In *HotSec*, 2011.
- [11] L. Cai and H. Chen. On the practicality of motion based keystroke inference attack. In S. Katzenbeisser, E. Weippl, L. Camp, M. Volkamer, M. Reiter, and X. Zhang, editors, *Trust and Trustworthy Computing*, volume 7344 of *Lecture Notes in Computer Science*, pages 273–290. Springer Berlin Heidelberg, 2012.
- [12] A. Charland and B. Leroux. Mobile application development: Web vs. native. *Commun. ACM*, 54(5):49–53, May 2011.
- [13] A. Das, N. Borisov, and M. Caesar. Exploring ways to mitigate sensor-based smartphone fingerprinting. *CoRR*, abs/1503.01874, 2015.
- [14] A. De Luca, A. Hang, E. von Zezschwitz, and H. Hussmann. I feel like i’m taking selfies all day!: Towards understanding biometric authentication on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI ’15, pages 1411–1414, New York, NY, USA, 2015. ACM.
- [15] W. Enck, P. Gilbert, S. Han, V. Tendulkar, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth. Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones. *Transactions on Computer Systems.*, June 2014.
- [16] Google. Location and sensors apis. Available at: [developer.android.com/guide/topics/sensors/index.html](http://developer.android.com/guide/topics/sensors/index.html).
- [17] M. Harbach, E. von Zezschwitz, A. Fichtner, A. D. Luca, and M. Smith. It’s a hard lock life: A field study of smartphone (un)locking behavior and risk perception. In *Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 213–230, Menlo Park, CA, July 2014. USENIX Association.
- [18] J. K. Hyungsub Kim, Sangho Lee. Exploring and mitigating privacy threats of html5 geolocation api. In *Annual Computer Security Applications Conference (ACSAC)*. New Orleans, Louisiana, USA, 2014.
- [19] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler. “my data just goes everywhere:” user mental models of the internet and implications for privacy and security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 39–52, Ottawa, July 2015. USENIX Association.
- [20] H. Khan, U. Hengartner, and D. Vogel. Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 225–239, Ottawa, July 2015. USENIX Association.
- [21] M. Mehrnezhad, E. Toreini, S. F. Shahandashti, and F. Hao. Touchsignatures: Identification of user touch actions based on mobile sensors via javascript (extended abstract). In *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2015)*. ACM, 2015.
- [22] M. Mehrnezhad, E. Toreini, S. F. Shahandashti, and F. Hao. Touchsignatures: Identification of user touch actions and pins based on mobile sensor data via javascript. *Journal of Information Security and Applications*, 26:23 – 38, 2016.
- [23] Y. Michalevsky, D. Boneh, and G. Nakibly. Gyrophone: Recognizing speech from gyroscope signals. In *Proc. 23rd USENIX Security Symposium*, 2014.
- [24] E. Miluzzo, A. Varshavsky, S. Balakrishnan, and R. R. Choudhury. Tapprints: your finger taps have fingerprints. In *Proceedings of the 10th international conference on Mobile systems, applications, and services*, pages 323–336. ACM, 2012.
- [25] M. F. Miller. A scaled conjugate gradient algorithm for fast supervised learning. *Neural Networks*, 6(4):525 – 533, 1993.
- [26] S. Narain, A. Sanatinia, and G. Noubir. Single-stroke language-agnostic keylogging using stereo-microphones and domain specific machine learning. In *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec ’14, pages 201–212, New York, NY, USA, 2014. ACM.
- [27] E. Owusu, J. Han, S. Das, A. Perrig, and J. Zhang. Accessory: password inference using accelerometers on smartphones. In *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications*, page 9. ACM, 2012.
- [28] A. Raij, A. Ghosh, S. Kumar, and M. Srivastava. Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI ’11, pages 11–20, New York, NY, USA, 2011. ACM.
- [29] L. Simon and R. Anderson. Pin skimmer: Inferring pins through the camera and microphone. In *Proceedings of the Third ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*, SPSM ’13, pages 67–78, New York, NY, USA, 2013. ACM.
- [30] R. Spreitzer. Pin skimming: Exploiting the ambient-light sensor in mobile devices. In *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*, SPSM ’14, pages 51–62, New York, NY, USA, 2014. ACM.
- [31] T. Watanabe, M. Akiyama, T. Sakai, and T. Mori. Understanding the inconsistencies between text descriptions and the use of privacy-sensitive resources of mobile apps. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 241–255, Ottawa, July 2015. USENIX Association.
- [32] K. Y. W. D. H. Y. G. N. P. Xing Jin, Xunchao Hu. Code injection attacks on html5-based mobile apps: Characterization, detection and mitigation. In *Proc. 21th ACM Conference on Computer and Communications Security*, 2014.
- [33] Z. Xu, K. Bai, and S. Zhu. Taplogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors. In *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, pages 113–124. ACM, 2012.

## APPENDIX

### Interview Script

Hi. Thanks very much for contributing to our study. In this interview, we will ask you to fill in a few questionnaires about mobile sensors such as GPS, camera, light, motion and orientation. You are encouraged to think out loud as you go through, and please feel free to provide any comments during the interview. There is no right or wrong answer, and our purpose is to evaluate the mobile sensors, not you. Everything about this interview is anonymous. Please provide some information about yourself in Table IV.

Age	
Gender	
Profession/ background (optional)	
1st language (optional)	
Mobile device	
Duration of owning a smartphone/tablet	

TABLE IV  
DEMOGRAPHY

## PART ONE

A list of multiple mobile sensors is presented below. To what extent do you know each sensor on a mobile device? Please rate them in the table (Table V was used).

## PART TWO

Imagine that you own a smartphone which is equipped with all these sensors. Consider this scenario: you have opened a game app which can have access to all mobile sensors. You leave the game app open in the background, and open your banking app which requires you to enter your PIN.

Do you think any of these sensors can help the game app discover your entered PIN? To what extent are you concerned about each sensor's risk to your PIN? Please rate them in the table (Table VI was used). In this section, please only rely on the knowledge you already have about the sensors, and if you do not know some of them, describe your feeling of security about them.

## PART THREE

Let us explain each sensor here:

- GPS: identifies the real-world geographic location.
- Camera, Microphone: capture pictures/videos and voice, respectively.
- Fingerprint, TouchID: scans the fingerprint.
- Touch Screen: enables the user to interact directly with the display by physically touching it.
- WiFi: is a wireless technology that allows the device to connect to a network.
- Bluetooth: is a wireless technology for exchanging data over short distances.
- NFC (Near Field Communication): is a wireless technology for exchanging data over shorter distances (less than 10 cm) for purposes such as contactless payment.
- Proximity: measures the distance of objects from the touch screen.
- Ambient Light: measures the light level in the environment of the device.
- Ambient Pressure (Barometer), Ambient Humidity, and Ambient Temperature: measure the air pressure, humidity, and temperature in the environment of the device, respectively.
- Device Temperature: measures the temperature of the device.
- Gravity: measures the force of gravity.
- Magnetic Field: reports the ambient magnetic field intensity around the device.
- Hall sensor: produces voltage based on the magnetic field.
- Accelerometer: measures the acceleration of the device movement or vibration.
- Rotation: reports how much and in what direction the device is rotated.
- Gyroscope: estimates the rotation rate of the device.
- Motion: measures the acceleration and the rotation of the device.

- Orientation: reports the physical angle that the device is held in.
- Sensor Hub: is an activity recognition sensor and its purpose is to monitor the device's movement.

Please feel free to ask us about any of these sensors for more information.

Now that you have more knowledge about the sensors, let us describe the same scenario here again. Imagine that you own a smartphone which is equipped with all these sensors. You have opened a game app which can have access to all mobile sensors. You leave the game app open in the background, and open your banking app which requires you to enter your PIN.

Do you think any of these sensors can help the game app to discover your entered PIN? To what extent are you concerned about each sensor's risk to your PIN? Please rate them in the table (Table VI was used). In this part, please make sure that you know the functionality of all the sensors. If you are unsure, please have another look at the descriptions, or ask us about them.

Thanks very much for taking part in this study. Please leave any extra comment here.

An Amazon voucher and a business card are in this envelope. Please contact us if you have any questions about this interview, or are interested in the results of this study.

Sensor	I've never heard of this	I've heard of this but I don't know what this is	I know what this is but I don't know how this works	I know generally how this works	I know very well how this works
Bluetooth					
Gyroscope					
GPS					
Sensor Hub					
Ambient Temperature					
Accelerometer					
Magnetic Field					
Motion					
Fingerprint					
Orientation					
Proximity					
Ambient Pressure					
Hall Sensor					
Rotation					
Touch Screen					
Camera					
TouchID					
Barometer					
Gravity					
Microphone					
Ambient Humidity					
WiFi					
Ambient Light					
NFC					
Device Temperature					

TABLE V  
THIS FORM WAS USED FOR PART ONE

Sensor	Risk to PIN				
	Not Concerned	A little Concerned	Moderately Concerned	Concerned	Extremely Concerned
Bluetooth					
Gyroscope					
GPS					
Sensor Hub					
Ambient Temperature					
Accelerometer					
Magnetic Field					
Motion					
Fingerprint					
Orientation					
Proximity					
Ambient Pressure					
Hall Sensor					
Rotation					
Touch Screen					
Camera					
TouchID					
Barometer					
Gravity					
Microphone					
Ambient Humidity					
WiFi					
Ambient Light					
NFC					
Device Temperature					

TABLE VI  
THIS FORM WAS USED FOR PARTS TWO AND THREE

# Exploring Psychological Need Fulfillment for Security and Privacy Actions on Smartphones

Lydia Kraus, Ina Wechsung, Sebastian Möller

Quality and Usability Lab, Telekom Innovation Laboratories, Technische Universität Berlin  
Email: {lydia.kraus, ina.wechsung, sebastian.moeller}@tu-berlin.de

**Abstract**—Much work has been conducted to investigate the obstacles that keep users from using mitigations against security and privacy threats on smartphones. By contrast, we conducted in-depth interviews ( $n = 19$ ) to explore users' motivations for voluntarily applying security and privacy actions on smartphones. Our work focuses on analyzing intrinsic motivation in terms of psychological need fulfillment. Our findings provide first insights on the salience of basic psychological needs in the context of smartphone security and privacy. They illustrate how security and privacy actions on smartphones are motivated by a variety of psychological needs, only one of them being the need for *Security*. Moreover, the results illustrate how psychological needs can help to explain the adoption of security and privacy technologies and the interaction with those technologies. We further discuss how the design of security and privacy technologies could be guided by the gained knowledge.

**Keywords:** Security and privacy; smartphones; psychological needs; user experience; user behavior

## I. INTRODUCTION

Smartphones are an extensive source for positive user experiences: using a smartphone allows people to stay connected, to consume new games and media, or to “quantify themselves” with fitness and health monitoring apps.

While smartphones offer vast opportunities for positive experiences, threats to users' security and privacy emerge at the same time. Those include malicious apps, data loss, surveillance, and profiling, just to name a few.

Related work indicates that users are concerned about many of these threats and about their privacy on smartphones [1], [2], [3]. To mitigate these threats there is a variety of actions users can take [4]. Former works suggest to gain further insights into security and privacy aspects from an end-user perspective by using experiential approaches [5], [6]. In this context

experience is seen as a holistic and broad view on the matter in order to gain a rich understanding of people's practices and lives [6]. Accordingly, while much work has been conducted to understand users' perceptions of smartphone security and privacy in terms of understanding [7], concerns [2], awareness [3], [8], attitudes [1], and feelings [9], we suggest using an experiential approach based on psychological needs to gain a deeper understanding of the matter.

User eXperience (UX) is a field of study which emerged between the mid-nineties and the turn of the millenium. In contrast to usability, which is mainly concerned with the functional aspects of technology usage, UX includes non-functional factors such as beauty and affective aspects of HCI [10]. Accordingly, UX is a multi-dimensional construct with a holistic view on the perceived product qualities (beyond usability), users' emotions, motivations, usage situations, and other dimensions (for a literature review of UX dimensions and study methods refer to [10]).

In our paper, we focus on the motivational dimension of user experiences in terms of psychological need fulfillment. Psychological needs have been suggested in several theories as an explanation for human behavior: for instance, self-determination theory suggests basic psychological needs as the fundamental mechanism for self-motivation [11]. Furthermore, it has been shown that need fulfillment is related to satisfying events and positive affect [12]. In the context of user experience research, Hassenzahl et al. [13] show that the main motivation to use an interactive technology is the fulfillment of psychological needs; a positive user experience is thus the result of need fulfillment [13].

A user for instance makes a phone call to experience the feeling of being close to others (thus, the motivation would be the fulfillment of the need *Relatedness*), rather than for the call's sake (example taken from [14]). Or, a user activates the privacy setting in a messaging app so that the sender of the messages cannot see when a message was read. This avoids the pressure to reply immediately to a message. In this case, the privacy setting is used to fulfill the basic psychological need of *Autonomy*. Psychological need fulfillment is a primary goal which all users have in common, the instantiation of the primary goal - the experience - is however highly context-dependent and subjective [14].

The goal of this paper is to learn about the psychological needs which users intend to fulfill with security and privacy actions on smartphones. We conducted semi-structured in-depth interviews with 19 users to explore the security and privacy actions which users employ on their smartphones and the reasons for them. Our findings illustrate how a variety of psychological needs drive those actions, only one of them being the need for *Security*. This knowledge can help to establish a new design space for positive user experiences induced by security and privacy actions on smartphones (cf. also Section V).

#### Contributions:

- We explore the motivational factors for security and privacy actions on smartphones in terms of psychological need fulfillment.
- We discuss how psychological needs can support the explanation of user behavior related to the adoption of and interaction with security and privacy actions.
- We provide examples on how to include psychological needs in the design of security and privacy technologies on smartphones.

**Structure:** After detailing related work on security and privacy actions on smartphones, user experience, and psychological needs in Section II, the interview methodology is presented in Section III. The interview results are reported in Section IV and discussed in Section V. We further discuss possibilities to use psychological needs as a design inspiration for security and privacy mechanisms in Section V.

## II. RELATED WORK

Much work has been conducted to describe user practices, concerns, and usability issues related to smartphone security and privacy. Despite the known usability issues of security mechanisms, users report being interested in applying further such mechanisms [15]. In the following, an overview of the main security and privacy actions users could deploy on their smartphone is presented. Those actions were also covered in the interviews which were conducted for this paper.

### A. Usability and adoption of smartphone security and privacy mechanisms

Scrutinizing app permissions is an indispensable action to avoid privacy intrusions and security issues on smartphones [4]. In the past, the implementation of the permission model differed between smartphone operating systems (OSes): Whereas iOS users were shown a permission-request as soon as an app requested it for the first time, android users had to accept all permissions or groups thereof before an app could be installed. In this implementation, Android permissions showed to be difficult to understand for users; also, the permission requests were shown at an unfavorable point in the decision making process, that was when the decision to install an app has already been made [7]. Several solutions have been suggested to increase the understanding of and the

attention towards permissions including improved information presentation and risk communication (cf. e.g. [16], [17], [18], [19]). In 2014, the Android permissions were grouped and their presentation was modified to include icons for each group. While this improved information presentation, security concerns remained [20]. The newest Android version (6.0), released in 2015, enables users to grant or not to grant single permissions for each app [21]. However, as of March 2016, Android 6.0 still has a negligible market share (2.3%) in the studied population [22]. Thus, the above described issues are still relevant.

A method to protect a smartphone from unauthorized access and subsequent privacy intrusions or security issues is the deployment of a screen lock together with an authentication method, such as a password or a PIN [4]. However, unlocking a smartphone with an authentication mechanism is time-consuming [23]. In a study of 2011, the PIN was perceived as a reliable method for protecting a mobile phone by only a quarter of users (26%) [15]. Nevertheless, as of 2014, many users are using a PIN or password to protect their device: 66% of users in Germany use a screen lock with a password [24]. A viable alternative to knowledge-based authentication methods are biometric methods such as Touch ID on iPhones and face unlock on Android devices [25]. Biometric methods, however, also rely on PINs or passwords for fallback authentication.

Regarding communication, eavesdropping and interception pose a threat. They can be mitigated by deploying end-to-end encryption of communication (calls and/or messages) [26]. Only recently, Whatsapp, one of the most popular instant messaging services for Smartphones, has announced the implementation of end-to-end encryption which is activated by default [27]. However, the usage of instant messaging services is not only accompanied by the risk of being eavesdropped, but also by the risk of privacy intrusions by other users. The latter can be counteracted by appropriate privacy settings. For instance, Rashidi and Vaniea report that many users actively use the privacy settings of Whatsapp - in a survey among Saudi Arab users almost a third of the respondents hid their last seen notice [28].

Another security threat, malware, might be mitigated by antivirus apps which can be easily installed for Android; however, their usefulness is questionable [29]. Likewise, the usage of security software is considered by many users as nonessential [3]. Keeping the device up-to-date is another mitigation strategy against malware. However, in a case study on update installation behavior, many users of an Android app did not immediately install updates - a behavior which may result in security vulnerabilities [30].

Threats may also arise from the device being unavailable due to denial of service attacks or exhausted battery power [26]. For counteracting the former, a resource management solution may be installed; these kind of applications are, however, difficult to implement [26]. A study by Chin et al. also showed that users worry about limited battery lifetime [1] when asked about concerns related to smartphone usage.

Data loss due to device loss or theft can be easily mitigated



by backups. While users are concerned about the latter threats [1], other tools to mitigate negative consequences in case of theft or loss such as remote data wipe, device locators and device encryption are poorly adopted [3]. This might be due to unawareness towards the existence of such features [1].

Chin et al. conducted a detailed study of users' practices on smartphones and their perception of security and privacy [1]; they found that users worry about the threats of physical theft or damage, data loss and insufficient back up, malicious apps and wireless network attackers, limited battery lifetime, and signal strength. Users' practices to protect from those threats may however have limited effectiveness. In some cases users deduce trust indications from indicators not meant as such. For instance, much value is put on other users' reviews in the app repository [1]. Kraus et al. investigated in a qualitative study which threats and mitigations on smartphones are known to users and how they perceive them: users reported different feelings including social pressure, helplessness, dependency, and fatalism [9]. They suggest that the reasons for those negative feelings may be grounded in a lack of psychological need fulfillment. Nevertheless, in their study, the use of self-reported mitigations was related to positive feelings such as trust and feelings of being able to exercise control<sup>1</sup> [9].

Related work suggests that users worry about threats to their security and privacy on smartphones and that many users are willing to adopt mitigations. However, usability shortcomings of mitigation technologies on smartphones and users' mixed feelings regarding threats and mitigations call for an approach that focuses on new methods to enable positive user experiences when applying security and privacy actions.

### B. Experiential approach to security and privacy

The necessity to include principles from user experience research into the design of security and privacy technologies has been recognized before. For example, Bødker et al. suggest that experiential approaches should be used to understand user behavior in the IT-security domain [5]: "In daily life, people rarely do activities solely for the purpose of security. Instead, most IT-security decisions are part of other activities with other purposes. When analyzing these use situations it is impossible to isolate IT-security tasks or decisions." Hence, security is dependent on context and usage motives, and not only on a secure device and the implemented security procedures [5]. By gaining an understanding of users' motivation in terms of psychological needs, our paper sheds lights on this issue.

Dunphy et al. [6] note that experience design faces a special challenge when it comes to security and privacy applications as within those applications two kind of users need to be taken into account: the target user and the adversary; moreover, a user might switch between being a targeted person and being an adversary depending on the context. For example,

<sup>1</sup>Note, that the actual and perceived security of what users consider to be a mitigation can vary greatly and will not be discussed at this point.

users can become adversaries when they start intruding the privacy of people with whom they interact in social networks. Gaining an understanding of target users' motivation in terms of psychological needs could also help to explain these kinds of situations.

### C. Psychological needs

Sheldon et al. [12] investigated the relationship between psychological needs and satisfying life events. They selected 10 psychological needs according to well-known theories of psychological need fulfillment (such as Deci and Ryan's self-determination theory [31], Epstein's cognitive-experiential self-theory [32]) and found that *Self-esteem*, *Autonomy*, *Relatedness* and *Competence* are the most salient needs in the context of satisfying life events. Their results were shown to be stable over time and across cultures.

Hassenzahl [14] took up the needs suggested by Sheldon et al. [12] and related them to a model of user experience. Psychological needs are used to describe classes of experiences [14]. This is done by considering different types of goals that underlie an action; do-goals and be-goals are differentiated [14]. Do-goals are derived from higher-level be-goals that are the fulfillment of an underlying need. A user, for instance, makes a phone call to experience the feeling of being close to others. Thus, the be-goal is feeling close to others (i.e. the fulfillment of the need *Relatedness*). The do-goal is the action of making the call (example taken from [14]). The fulfillment of psychological needs (the be-goal) leads to a positive user experience [13].

While psychological needs serve to describe motivational aspects and thus allow for making interpretations of users' behavior, they can also serve as an inspiration for product design [14], [33]. Studies show that need fulfillment can be manipulated through product features leading to a positive change in user experience evaluations [33], [34]. Also, users' judgement of a system's hedonic quality, i.e. quality aspects beyond the functional, is influenced by need fulfillment [14]. However, this depends on the attribution, i.e. the degree to which users deem the product responsible for the experience [14].

The study presented in this paper is based on the needs as defined in Sheldon et al. [12]. The usefulness of this set of needs in the context of HCI has previously been shown by Hassenzahl et al. [13]. Fronemann and Peissner [33] also build upon a set of psychological needs defined by Sheldon et al. [12] and Reiss [35]. An additional need they define which is not covered by the definitions of Sheldon et al. [12] is *Keeping the meaningful* [33]. We too included this need into our study. In the following, definitions of the psychological needs which we used in our research are provided.

**Autonomy:** "Feeling like you are the cause of your own actions rather than feeling that external forces or pressures are the cause of your actions." [12]

**Competence:** "Feeling that you are very capable and effective in your actions rather than feeling incompetent or

ineffective.” [12]

**Relatedness:** “Feeling that you have regular intimate contact with people who care about you rather than feeling lonely and uncared for.” [12]

**Self-actualization:** “Feeling that you are developing your best potentials and making life meaningful rather than feeling stagnant and that life does not have much meaning.” [12]

**Security:** “Feeling safe and in control of your life rather than feeling uncertain and threatened by your circumstances.” [12]

**Popularity:** “Feeling that you are liked, respected, and have influence over others rather than feeling like a person whose advice or opinions nobody is interested in.” [12]

**Money/Luxury:** “Feeling that you have plenty of money to buy most of what you want rather than feeling like a poor person who has no nice possessions.” [12]

**Physical/Bodily:** “Feeling that your body is healthy and well-taken care of rather than feeling out of shape or unhealthy.” [12]

**Self-esteem:** “Feeling that you are a worthy person who is as good as anyone else rather than feeling like a ‘loser’.” [12]

**Stimulation:** “Feeling that you get plenty of enjoyment and pleasure rather than feeling bored and understimulated by life.” [12]

**Keeping the meaningful:** “Collecting meaningful things” [33]/“saving” [35]

### III. METHODOLOGY

Following the description of be-goals and do-goals, psychological needs are related to the question why something is done whereas actions are related to the question what is done and how it is done [14]. Therefore the script for the semi-structured in-depth interviews concerned the following research questions:

- Which security and privacy actions are employed by smartphone users? (*What?*)
- How are they employed? (*How?*)
- Why are they employed? (*Why?*)

The interview script can be found in the appendix of this paper. With this approach participants were not explicitly asked for the needs they aim to fulfill with their actions. Therefore, we considered the why-questions to provide answers regarding the reasons for doing an action and we coded those reasons with the psychological needs.

The interview script covered a variety of possible actions, extracted from the literature on smartphone security risks [4], [26] and users’ threat perception [1]. Action-questions were intentionally designed in an open manner as we did not want to assume that users only stick to the actions which are defined in the literature. The salience of the topics security and privacy increased during the course of the interview.

The interview was divided into three parts. In the first part, participants were asked about their general smartphone usage habits, e.g. reasons why they bought a smartphone, which operating system they use, and if they have used another operating system before. Then they were asked about smartphone sharing and usage at work. Afterwards, several

questions on app usage, app installing, and uninstalling were asked. Some of the questions were taken from [1].

In the second part of the interviews, the central themes were security and privacy actions, including questions about the first time that participants set up their smartphone, usage of data connections, installing of updates, usage of pre- and postpaid options, battery consumption, theft protection, backups, internet usage, financial functions, protection from app access to sensitive information and communication.

In the third part, questions covered security and privacy software usage, password lock usage, and thoughts on general threats of smartphone usage. For each question of the interview, the interviewers were instructed to ask follow-up questions on reasons and triggers for behavior.

#### A. Procedure

The interviews were conducted in German in the beginning of 2015 at our lab. Each interview was conducted by one interviewer. To reduce interviewer effects, there were two interviewers. Approximately half of the interviews were conducted by Interviewer 1, the other half by Interviewer 2. Audio recordings were taken to enable verbatim transcription after the interviews. The audio recordings were deleted after the transcription process. The sessions took between 20 and 40 minutes depending on how talkative the participants were. Participants received 12 EUR reimbursement. At the beginning of the interview, participants received an information sheet and were asked for consent. Then, questions on demographics, smartphone usage (frequency of use, etc.), privacy concern and ICT attitudes were presented to the participants. During the recruitment we did not mention that the interview is about security and privacy, but we told the participants that we are interested in their smartphone usage habits.

At the end of the interviews the participants were thanked and debriefed. Due to the nature of the interview it might have been that the participants became aware of shortcomings in their security behavior. Therefore, after the interview, they were provided with a flyer on which they could find further information on how to protect their security and privacy on smartphones.

#### B. Analysis

The codebook consisted of the descriptions of the 11 psychological needs (cf. Section II), the items of the need fulfillment questionnaire [12], and a few items of the UNEEQ questionnaire (only for *Keeping the meaningful*) [36]. Thus, the codes could be used for either need fulfillment or frustration.

Two coders independently coded the interviews by applying the codebook described above. Interrater-agreement between the two coders was found to be moderate (Cohen’s  $\kappa = 0.46$ ) according to Landis and Koch [37]. The disagreements between the coders stemmed from a few issues. During the coding, the coders came across many passages in which participants told that they would do an action in order to save money. However, saving money is not explicitly part

of the definition of the need *Money/Luxury* as described in Section II. Nevertheless, in most passages related to saving money, participants were willing to corrupt their privacy or security in order to get access to nice possessions. For instance, they said that they would choose the free version of an app rather than the paid version, although the free version required more permissions. Thus after discussion, the coders decided to label these passages as *Money/Luxury*. The coders also discussed about the *Security* code. This code was rather found in the context of *being safe from threats* than *having a need for structure or control*. The coders agreed that the first definition is valid as it can be found in the questionnaire on need fulfillment [12]. There was also disagreement on whether situations in which the participants reported the desire that others cannot track or observe them should be coded as *Security* or *Autonomy*. This is a typical situation related to privacy; however, a need for privacy is not part of the needs suggested in the related literature (cf. Section II). In the end, the coders agreed on coding these passages as *Autonomy* - in line with Westin's definition of the functions of privacy, one of them being personal autonomy [38]. In the following we use the coded transcripts upon which the coders finally agreed.

Additionally to the analysis of the psychological needs, a list of security and privacy actions was extracted from the data by the coders. Actions in the list include actions as defined in the literature [4], [26] and actions which were additionally mentioned by the participants. Based on this list, the coders analyzed independently whether an action was applied by a participant or not. For the coding of the actions, the coders reached almost perfect interrater-agreement (Cohen's  $\kappa = 0.84$ ) according to Landis and Koch [37]. The coders met to discuss disagreements and to reach consent. Table I reports the results upon which the coders agreed.

### C. Participants

19 smartphone users (10 female) were recruited from a panel of our institution. The age ranged from 18 to 58 years with an average of 31 years. Participants had diverse educational levels (approximately equally distributed among secondary school degree, qualification for university entrance, and university degree). Among the sample were 9 employees, 7 students and 3 job seekers.

### D. Smartphone usage

There were 13 Android users, 5 iPhone users and 1 Windows Phone user. The sample roughly reflects the distribution of smartphone operating systems among the smartphone user population in Germany at the time of the study (Android 70%, iOS 20%, Windows Phone 5%) [39]. Smartphone usage experience among the participants was diverse: 4 participants had owned their smartphone for less than a year, 7 for 1-3 years and 8 for more than 3 years. Most of the participants use their smartphone at least once per hour (N=15). Only one participant had a professional IT background.

## IV. RESULTS

Participants reported the application of many security and privacy actions. Those actions largely rely on either mindfulness or pre-installed mechanisms. The psychological needs motivating the application of the reported actions are diverse: besides *Security* which was likely to be a motivator due to the nature of the interview, *Autonomy* and *Money/Luxury* play a major role. *Competence*, *Relatedness*, and *Stimulation* were found to be of moderate importance. *Keeping the meaningful* and *Popularity* were only relevant for a few actions. *Self-actualization*, *Physical/Bodily*, and *Self-esteem* were found to play a minor role as motivators.

The results of the psychological need analysis are structured according to the macro-structure of the interview script. For each subsection, the 2-3 most mentioned needs are discussed.

### A. Security and privacy actions

An overview of the reported actions is provided in Table I. Saving battery lifetime was reported most frequently, followed by switching off all data connections, deploying updates and protecting the device from theft.

Neither the installation of nor the subscription to additional apps or services is required for the 10 top strategies as those strategies are either based on mindfulness or on pre-installed security/privacy mechanisms. Examples for the latter include screen lock with authentication or backups to the cloud (if the backup app was pre-installed).

Note, that actions encompass what the participants have reported, not what they may actually use. For example, iPhone users may not have been aware that encryption on iOS is enabled by default when using a screen lock with authentication. Further note, that end-to-end encryption was not implemented in many messaging apps by the time of the study. Thus, the use of messaging apps with end-to-end encryption was interpreted as a separate action. Table I does not take into account intensity and frequency of the deployed actions. For example, for "checking permissions" there may be participants who check app permissions everytime, while other participants may only check them when they are suspicious for some reason.

In the following we report the psychological needs related to the different actions.

### B. Saving battery lifetime

From an IT-security perspective the (automatic) monitoring of battery consumption may be used to detect malicious activities on a device [26]. While users could also regularly check their battery status to detect apps that unnecessarily drain energy, the participants in our study mentioned checking their battery status as a safety measure: they reported to save battery lifetime to be, for example, available for friends. Thus, *Relatedness* is one reason for saving battery lifetime. P12 mentioned that he started to check his battery status regularly as there have been situations where "I was somehow absent-minded and my battery only had 30%, but I was somewhere

Security and privacy actions	freq.	%
Save battery lifetime	18	95%
Switch off all data connections (e.g. by flight-mode)	17	89%
Deploy updates	16	84%
Protect from theft (e.g. by securely storing the device)	14	74%
Check permissions	14	74%
Make backups	14	74%
Use screen lock with authentication	12	63%
Avoid financial apps/ functions (e.g. online banking)	10	53%
Check monthly bill/ prepaid balance	9	47%
Disable WiFi connection	6	32%
Disable Bluetooth	5	26%
Disable GPS	4	21%
Hide one's identify (e.g. by fake user profiles)	4	21%
Reduce online "data traces"	3	16%
Adjust privacy settings of messaging apps	3	16%
Use antivirus apps	3	16%
Log out from services	3	16%
Take out insurance	3	16%
Use remote management apps	3	16%
Do not use messaging apps	2	11%
Use apps for privacy protection/ permission management	2	11%
Use messaging apps with end-to-end encryption	2	11%
Modify privacy settings of the device	1	5%
Uninstall pre-installed apps	1	5%
Root the device	1	5%
Do not download apps at all	1	5%
Use data/ device encryption	0	0%

TABLE I

SELF-REPORTED SECURITY AND PRIVACY ACTIONS. PERCENTAGES DO NOT SUM UP TO 100 AS PARTICIPANTS COULD REPORT SEVERAL ACTIONS.

outside for let's say five or six hours; well, I need to be available for friends or so."

Another reason for saving battery lifetime is *Security*, as evident in the statement by P9: "Mhm well, in fact [...] it happens quite often, that I need to find my way home via Google Maps or public transport and therefore I always want to have at least 10% battery left and that's why... that's why I save battery".

### C. Connectivity

When we asked the participants about situations in which their data connections such as Bluetooth, NFC or GPS are disabled, we expected that they report on turning off WiFi for example in order to avoid network attacks. Instead, most of the participants mentioned situations in which they switch off all data connections (e.g. by activating the flight mode). This behavior is driven by the need for *Autonomy*: "I don't need to be available all the time, well, I can be without my mobile phone" (P11). "Because I want to be let alone" (P9). "I always disabled it [all data connections] at work, so that I don't get distracted" (P15). *Money/Luxury* is another reason why data connections are switched off. P17 noted: "[...] when I am at home then I use WiFi and switch off my mobile internet, because I think I can save some of my data contingent doing so at least that is how I understood it." However, for few participants, a need for *Security* was found related to the usage of public WiFi spots: "Well, for me that is... open WiFi is too risky for me." (P15)

### D. Updates

Updates were seen as a source for *Stimulation* rather than a necessity in terms of *Security*, for instance by P8: "Yes, if there are new updates I install them so that I have the latest version [of an app]." Doing updates manually provides *Autonomy* for some of the participants: "In certain intervals, maybe once per month, I enter Google Play and then I check which apps I have [on my phone] and for which of those apps updates are needed. Then I decide what I update or what I don't update" (P2).

### E. Protection from theft

Interestingly, instead of using remote management apps or the like, many of the participants mentioned that they store their device securely or that they pay attention to where they leave the device. This provides them with a feeling of *Security*, as can be seen in the quote by P15: "It's always strange, when it [the phone] is somewhere else, for example in my backpack; I'd rather carry it on me, then I know it's there and I notice relatively quickly if it would be gone." P12 stated: "I just do it [storing it securely] as a preventive measure, just not to be placed in such a situation [that the phone is stolen]."

### F. Screen lock with authentication

Not surprisingly, most quotes related to screen locks with authentication were coded with *Security*, an example is the following quote by P8: "Uumh, if it [the phone] is stolen or so, [for the thief] it wouldn't be so easy to use it immediately." P6 noted as a reason to use password lock: "I believe that it's maybe... In case that one loses the phone, it is a bit more difficult [to access it]." *Security* and *Popularity* as reasons to adopt a password lock were mentioned by P5: "In the beginning it was, because I thought it is pretty cool how my friends typed in their security codes on their mobile phone. Now it is just for security reasons." Thus, for P5 locking mechanisms have the potential to convey the impression of being "cool" to others.

### G. App selection, uninstalling apps and mitigating access to sensitive information

When it comes to app selection *Stimulation* plays a major role as noted by P11: "sometimes I check the category 'newest apps' and those that sound interesting will be downloaded." Also, the influence of the price, i.e. *Money/Luxury*, was mentioned by several participants, for instance in this quote: "Well, there are enough [apps] for free" (P17).

*Security* may be a decision factor in the app selection process, as noted by P3: "It depends on what kind of app it is, how urgent do I need that app? Well, if I want to download some game just for fun and [then I] see 'Okay, the App wants to have access to everything', [...] than I just dont install it." P4 mentions *Security* concerns during app selection: "[...] but then sometimes I do worry, a self-employed developer, what kind of mischief they could do."

A feeling of not being *competent* when it comes to judging permissions was expressed by P7: "Therefore I don't see

myself in the position, to switch those things [the permissions] off; I think that I am allowing it [having access] to some apps.”

*Autonomy* is experienced by not allowing apps to access location data “[I switch off GPS] because I do not want, that someone who should not know it, knows where I am.” (P11). When it comes to uninstalling apps, *Autonomy* is a reason, as evident from this statement by P12: “Simply because I don’t want Apple to know where I am or something like that”. However, also *Money/Luxury* may be a reason for uninstalling an app: “Well, sometimes there are apps which are advertised to be free of charge and then you only got a couple of functions and you have to pay for many other functions. And well then I rather uninstall those apps because it annoys me.” (P13).

#### H. Backups

*Security* and *Keeping the meaningful* were the only reasons that were salient in the context of backups: “Yes, because the data on my mobile phone is important to me... and well it is better... safety comes first.” (P8). Unsurprisingly, the desire to keep (meaningful) things is related to the subjective value that the participants attach to them, as implied by this statement by P3: “Well, I am a person who loses his mobile phone quite often, and, well I was in Brazil and took some pictures there. And after two weeks of traveling I dropped my mobile phone in a river. Well, then I thought ‘mhh damn it’. I got my phone to work again, but then I uploaded everything to the cloud well, so that I do not lose all my pictures [...]”

#### I. Communication

Being in contact with people one cares about, i.e. *Relatedness*, was mentioned by many of the participants as a reason for using messaging apps: “The reason for using it [WhatsApp] is actually that all my friends are using it, otherwise I would like to use another one [app].” (P9). “Because everyone used to use it and if you did write an SMS, then you were kind of out and well then you just used it too. Last year I tried to get rid of WhatsApp, but there are still too many people who still got it and won’t write SMS and well then you just have to get back to WhatsApp.” (P15).

When we asked the participants if they do something in order to protect their communication, we expected that they would mention end-to-end encryption or the like. However, only one participant reported to use it. Instead many said that they use privacy settings in messaging apps. We labeled these statements with *Autonomy*: “I wouldnt describe it as a protection measure, but for WhatsApp I turned off, that you can see when I was online the last time or stuff like that... well.” (P3). Group chats in messaging apps were seen as a possible source of unpleasant consequences by P6: “Yes, so, I am careful when it comes to these group... group-chats or things like that. I do not use them, because I think they are quite precarious [...]” Therefore, this quote was coded with *Security*.

Summarizing, we found a variety of examples how psychological needs, i.e. be-goals, drive security and privacy

actions on smartphones: for instance, the participants reported *Relatedness* and *Security* as motivators for saving battery lifetime; they further reported that *Autonomy*, *Money/Luxury*, and *Security* are playing a role in managing connectivity; they also mentioned that *Stimulation* and *Autonomy* motivate actions related to updates and that the need for *Security* motivates the protection from theft; *Security* was mainly mentioned as motivator for using a screen lock with authentication, however, there is also a potential for *Popularity* being addressed with this action. App selection was noted to be driven by *Stimulation* and *Money/Luxury*, whereas *Security*, *Competence* (or a lack thereof) and *Autonomy* were reported to be related to uninstalling apps and mitigating access to sensitive information. The interviews further indicated that backups are motivated by *Keeping the meaningful* and the need for *Security*; communication is related to *Relatedness*, whereas its protection is related to *Autonomy*, and *Security*, both rather in the context of threats arising from other users.

## V. DISCUSSION

Our findings indicate that users apply diverse security and privacy actions to protect themselves from threats on their smartphones. Quantifying the effectiveness of these actions is out of the scope of this paper. However, the mere finding suggests a huge design space for future security and privacy technologies. Our results further illustrate how a variety of psychological needs drive security and privacy actions on smartphones. How psychological need fulfillment can be included into the design of security and privacy technologies, is discussed in the following.

#### A. Limitations

Our study is of qualitative nature, thus, we do not aim to infer any statements on the importance of each need for each action. Need fulfillment is on the one hand context-dependent. On the other hand, there may be some needs which are especially important for specific actions. Quantifying them is subject to quantitative studies, for which our paper provides a profound basis.

The interviews were annotated with predefined concepts from theories of psychological needs. This is a subjective process and it might be that some quotes could be interpreted in a different way. The moderate inter-rater agreement indicates that the application of psychological needs in the context of security and privacy on smartphones may profit from further conceptualization and specification. We leave additional conceptualizations to future work for which our paper provides a good starting point.

Our study sample consisted partly of students and job seekers which might have led to the result that saving money was a rather salient motive in the decision making process. Despite this limitation, our sample reflects well the smartphone operating system distribution in the studied population. Studies aiming at quantifying and generalizing the results, should however, administer a sample which is representative w.r.t. to further population characteristics.

### B. Psychological needs as an explanation for user behavior

The results of the interviews indicate that a variety of psychological needs is salient in the context of security and privacy actions on smartphones. As psychological needs can be considered as high-level primary goals (“be-goals” [14]), our results provide insights into these primary goals and how they are aligned (or not) with security and privacy actions. For instance, backups may be motivated by the need for *Keeping the meaningful* rather than for the sake of *Security* only. A password lock for the smartphone screen may be used to achieve a feeling of *Security*, but it may be also motivated by the need for *Popularity*. This is the case when its usage is perceived as “trendy”. Data connections may be switched off for privacy reasons (i.e. *Autonomy*), but also for *Security* reasons or to save money (i.e. *Money/Luxury*). Using certain messaging apps may be motivated by the need for *Relatedness* rather than the need for *Security*, but the communication itself might be regulated through privacy settings whenever there is a need for *Autonomy*. App selection can in some cases be driven by the need for experiencing new things (i.e. *Stimulation*); in other situations users check the permissions thoroughly to avoid being surveilled by privately owned companies (i.e. the emphasis is on the need for *Autonomy*). Concerning communication, *Relatedness* is a motivator for the adoption of messaging apps and communication protection is driven by *Autonomy* and the need for *Security*.

Security or privacy are often considered as secondary goals [40]. However, one could have expected that for users of security and privacy actions on smartphones, security and privacy would be primary goals. Nevertheless, the interview results indicate that even for security and privacy actions the need for *Security* is only one primary goal among others. Which psychological need users intend to fulfill depends on the one hand on contextual factors. On the other hand, there may be groups of users with similar characteristics that intend to fulfill a specific need with a specific security and privacy action. We plan to conduct further studies to examine the relationships between context, user characteristics and psychological need fulfillment for security and privacy actions on smartphones.

### C. Using psychological needs in the security and privacy context

During the analysis of the psychological needs, we have made a number of assumptions regarding their interpretation. We have interpreted the desire for privacy as being related to *Autonomy*. Pedersen [41] and Westin [38] suggest that there is a variety of privacy behaviors which are driven by further functions (besides *Autonomy*) such as emotional release, self-evaluation, and limited and protected communication [38]. We suspect that including the privacy functions will lead to a better conceptualization of psychological needs in the context of security and privacy research. We plan to conduct further studies to investigate how the functions defined by Westin and Pedersen can be integrated into the concept of psychological needs. We further interpreted *Money/Luxury* to include the desire to save money. However, this desire could

be rather an extrinsic motivational factor than an intrinsic motivational factor (psychological needs are considered as intrinsic motivators). Thus, saving money may not lead per se to a positive user experience and may be rather a necessity than a reason. This issue should be considered in future studies.

### D. Psychological needs as design inspiration for security and privacy technologies on smartphones

Addressing psychological needs in security and privacy technologies for smartphones creates a new design space for such technologies. In the following, we provide examples on how security and privacy technologies that support psychological need fulfillment could look like.

1) *Authentication*: We suggest improving the user experience of password locks by addressing additional needs besides *Security* such as *Stimulation* (e.g. by making unlocking fun) or *Popularity* (by having a “cool” screen lock). There are a few examples for addressing *Stimulation* in terms of joy during authentication: related work shows that for instance gesture-based authentication is able to evoke different positive emotional outcomes. Aumi et al. [42] present an authentication system which is based on in-air gestures performed in the vicinity of a portable device. In a user study they show that the gestures’ security is positively correlated with ratings of pleasantness and excitement. Moreover, Karlesky et al. [43] find full-body gestures for access control to provide a potential for interactions which are perceived pleasurable by users. *Popularity* in authentication mechanisms could be addressed by providing users with a “cool” authentication method. For example, Bhagavatula et al. find that fingerprint authentication on smartphones is perceived as “cool” [25]. Also, many solutions to improve usability of knowledge-based authentication methods have been suggested in the domain of graphical authentication [44]. It is subject to future research to investigate whether those solutions could provide for better need fulfillment and a positive user experience. Furthermore, we plan to investigate in future studies how psychological needs such as *Stimulation* and *Popularity* can be systematically addressed in the design of mobile authentication methods.

2) *Updates*: Participants in our study mentioned installing updates to get the newest version of an app. By definition, experiencing new things is associated with the need for *Stimulation*. However, this applies only if the new experience is positive. Vaniea et al. [45] show that users become frustrated when installing updates that feature new user interfaces that interrupt the users’ normal workflow. Thus, updates are a two-edged sword: on the one hand they are able to positively surprise users when new functionalities or features are added to an app, thus addressing the need of *Stimulation*. On the other hand, users who have had bad experiences with installing updates may refrain from installing them in the future which may lead to security vulnerabilities [45]. One option to avoid negative effects on users’ security behavior is to separate security updates from other updates [46]. Thereby, in the best case, users will not experience any changes after installing a security update. Nevertheless, it may also be the case, that

updates just for security purposes are not deployed. Thus, an approach based on psychological need fulfillment could be to motivate users to install security updates by connecting these updates with stimulating experiences. For instance, appraisal messages could be shown or gamification approaches could be used to achieve such experiences. How approaches that address psychological needs in update messages could look like in detail, is an interesting research question for future studies.

3) *App Permissions*: Not only in our study, app permissions proved to be hard to understand by some of the participants (cf. also [7]). As a consequence, the psychological need of *Competence* may be deprived. On the other hand, our results suggest that users appreciate having the possibility to autonomously select which permissions they grant (for instance with respect to location data). Providing users with a clear context to make a decision is in any case recommendable [40]. Related work also indicates that a clear context supports security-friendly decisions when granting permissions [17], [18]. Whether this approach is also capable to address users' need for *Competence* and inducing a positive user experience is a subject for future studies. Another worthwhile topic for future studies is to investigate to which degree run-time permissions (as currently featured in iOS and Android 6.0) are perceived as fulfilling the need for *Autonomy* without being annoying.

In summary, our results illustrate how psychological needs can be used as high-level primary goals for the explanation of user behavior related to security and privacy actions on smartphones; moreover, they provide new inspirations for the design of security and privacy technologies on smartphones. How the psychological needs can be systematically addressed in the design of security and privacy technologies on smartphones is an interesting research topic for future studies.

## VI. CONCLUSION

We conducted semi-structured in-depth interviews with 19 participants to investigate the psychological needs that drive security and privacy actions on smartphones. Our results show a variety of self-reported actions and illustrate how those actions are motivated by a variety of psychological needs, beyond the need for *Security*. Our results provide examples on how psychological needs can be used as high-level primary goals to explain user behavior related to the adoption of security and privacy actions on smartphones; furthermore, they provide design inspirations for new versions and future prototypes of security and privacy technologies. Our paper offers a basis for further conceptualizations and for elaborating on the potential that the application of psychological needs offer in the security and privacy context.

## VII. ACKNOWLEDGMENTS

This work was funded by the EU FP-7 support action ATTPS under grant agreement no. 317665. We would like to express our gratitude to Tobias Fiebig for his assistance in

preparing the interview study and to Maija Poikela for proof-reading the paper.

## REFERENCES

- [1] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, "Measuring user confidence in smartphone security and privacy," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 2012, p. 1.
- [2] A. P. Felt, S. Egelman, and D. Wagner, "I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns," in *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices*. ACM, 2012, pp. 33–44.
- [3] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? security awareness in smartphone platforms," *Computers & Security*, vol. 34, pp. 47–66, 2013.
- [4] G. Hogben and M. Dekker, "Smartphones: Information security risks, opportunities and recommendations for users," *European Network and Information Security Agency*, vol. 710, no. 01, 2010.
- [5] S. Bødker, N. Mathiasen, and M. G. Petersen, "Modeling is not the answer!: Designing for usable security," *interactions*, vol. 19, no. 5, pp. 54–57, Sep. 2012. [Online]. Available: <http://doi.acm.org/10.1145/2334184.2334197>
- [6] P. Dunphy, J. Vines, L. Coles-Kemp, R. Clarke, V. Vlachokyriakos, P. Wright, J. McCarthy, and P. Olivier, "Understanding the Experience-Centeredness of Privacy and Security Technologies," in *Proceedings of the 2014 workshop on New Security Paradigms Workshop*, 2014, pp. 83–94.
- [7] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 2012, p. 3.
- [8] L. Reinfelder, Z. Benenson, and F. Gassmann, *Trust, Privacy, and Security in Digital Business: 11th International Conference, TrustBus 2014, Munich, Germany, September 2-3, 2014. Proceedings*. Cham: Springer International Publishing, 2014, ch. Differences between Android and iPhone Users in Their Security and Privacy Awareness, pp. 156–167. [Online]. Available: [http://dx.doi.org/10.1007/978-3-319-09770-1\\_14](http://dx.doi.org/10.1007/978-3-319-09770-1_14)
- [9] L. Kraus, T. Fiebig, V. Miruchna, S. Möller, and A. Shabtai, "Analyzing end-users knowledge and feelings surrounding smartphone security and privacy," *S&P. IEEE*, 2015.
- [10] J. A. Bargas-Avila and K. Hornbæk, "Old wine in new bottles or novel challenges: a critical analysis of empirical studies of user experience," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2011, pp. 2689–2698.
- [11] R. M. Ryan and E. L. Deci, "Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being," *American psychologist*, vol. 55, no. 1, p. 68, 2000.
- [12] K. M. Sheldon, A. J. Elliot, Y. Kim, and T. Kasser, "What is satisfying about satisfying events? testing 10 candidate psychological needs," *Journal of personality and social psychology*, vol. 80, no. 2, p. 325, 2001.
- [13] M. Hassenzahl, S. Diefenbach, and A. Göritz, "Needs, affect, and interactive products—facets of user experience," *Interacting with computers*, vol. 22, no. 5, pp. 353–362, 2010.
- [14] M. Hassenzahl, "Experience design: Technology for all the right reasons," *Synthesis Lectures on Human-Centered Informatics*, vol. 3, no. 1, pp. 1–95, 2010.
- [15] N. Ben-Asher, N. Kirschnick, H. Sieger, J. Meyer, A. Ben-Oved, and S. Möller, "On the need for different security methods on mobile phones," in *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*. ACM, 2011, pp. 465–473.
- [16] P. G. Kelley, L. F. Cranor, and N. Sadeh, "Privacy as part of the app decision-making process," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2013, pp. 3393–3402.
- [17] M. Harbach, M. Hettig, S. Weber, and M. Smith, "Using personal examples to improve risk communication for security & privacy decisions," in *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2014, pp. 2647–2656.
- [18] L. Kraus, I. Wechsung, and S. Moller, "Using statistical information to communicate android permission risks to users," in *Socio-Technical Aspects in Security and Trust (STAT), 2014 Workshop on*. IEEE, 2014, pp. 48–55.



- [19] K. Benton, L. J. Camp, and V. Garg, "Studying the effectiveness of android application permissions requests," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2013 IEEE International Conference on*. IEEE, 2013, pp. 291–296.
- [20] C. Toombs, "Simplified Permissions UI in The Play Store Could Allow Malicious Developers To Silently Add Permissions," <http://www.androidpolice.com/2014/06/10/simplified-permissions-ui-in-the-play-store-could-allow-malicious-developers-to-silently-add-permissions/>, (accessed: 2016-02-06).
- [21] Android Developers, "Requesting Permissions at Run Time," <http://developer.android.com/training/permissions/requesting.html>, (accessed: 2016-05-04).
- [22] Statista - Das Statistikportal, "Anteil der verschiedenen Android-Versionen an allen Geräten mit Android OS weltweit im Zeitraum 01. März 2016 bis 07. März 2016," <http://de.statista.com/statistik/daten/studie/180113/umfrage/anteil-der-verschiedenen-android-versionen-auf-geraeten-mit-android-os/>, (accessed: 2016-04-25).
- [23] M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "It's a hard lock life: A field study of smartphone (un) locking behavior and risk perception," in *Symposium on Usable Privacy and Security (SOUPS)*, 2014.
- [24] Initiative D21 and Huawei Technologies, "Mobile Internetnutzung Gradmesser für die digitale Gesellschaft," [http://www.initiatived21.de/wp-content/uploads/2014/12/Mobile-Internetnutzung-2014\\_WEB.pdf](http://www.initiatived21.de/wp-content/uploads/2014/12/Mobile-Internetnutzung-2014_WEB.pdf), (accessed: 2016-04-25).
- [25] C. Bhagavatula, B. Ur, K. Iacovino, S. M. Kywe, L. F. Cranor, and M. Savvides, "Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption," *Proc. USEC*, 2015.
- [26] A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, and S. Dolev, "Google android: A state-of-the-art review of security mechanisms," *arXiv preprint arXiv:0912.5101*, 2009.
- [27] WhatsApp Blog, "end-to-end encryption," <http://blog.whatsapp.com/10000618/end-to-end-encryption>, 2016, (accessed: 2016-04-25).
- [28] Y. Rashidi and K. Vaniea, "Poster: A user study of whatsapp privacy settings among arab users," in *IEEE Symposium on Security and Privacy*, 2015.
- [29] R. Fedler, J. Schütte, and M. Kulicke, "On the effectiveness of malware protection on android," *Fraunhofer AISEC, Berlin, Tech. Rep.*, 2013.
- [30] A. Möller, F. Michahelles, S. Diewald, L. Roalter, and M. Kranz, "Update behavior in app markets and security implications: A case study in google play," in *Proc. of the 3rd Intl. Workshop on Research in the Large. Held in Conjunction with Mobile HCI*, 2012, pp. 3–6.
- [31] E. L. Deci and R. M. Ryan, "The 'what' and 'why' of goal pursuits: Human needs and the self-determination of behavior," *Psychological inquiry*, vol. 11, no. 4, pp. 227–268, 2000.
- [32] S. Epstein, "Cognitive-experiential self-theory. handbook of personality: theory and research/ed. perrin l. a," 1990.
- [33] N. Fronemann and M. Peissner, "User experience concept exploration: user needs as a source for innovation," in *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational*. ACM, 2014, pp. 727–736.
- [34] A. Sonnleitner, M. Pawlowski, T. Kässer, and M. Peissner, "Experimentally manipulating positive user experience based on the fulfillment of user needs," in *Human-Computer Interaction-INTERACT 2013*. Springer, 2013, pp. 555–562.
- [35] S. Reiss, "Multifaceted nature of intrinsic motivation: The theory of 16 basic desires," *Review of General Psychology*, vol. 8, no. 3, p. 179, 2004.
- [36] "Uneeq - user needs questionnaire," [http://www.hci.iao.fraunhofer.de/content/dam/hci/de/documents/UXellence\\_UserNeedsQuestionnaire\\_EN.pdf](http://www.hci.iao.fraunhofer.de/content/dam/hci/de/documents/UXellence_UserNeedsQuestionnaire_EN.pdf), (accessed: 2016-04-25).
- [37] J. R. Landis and G. G. Koch, "The measurement of observer agreement for categorical data," *biometrics*, pp. 159–174, 1977.
- [38] A. F. Westin, "Privacy and freedom, atheneum," *New York*, p. 7, 1967.
- [39] Statista - Das Statistikportal, "Marktanteile der Betriebssysteme an der Smartphone-Nutzung in Deutschland von Dezember 2011 bis Februar 2015," <http://de.statista.com/statistik/daten/studie/170408/umfrage/marktanteile-der-betriebssysteme-fuer-smartphones-in-deutschland/>, (accessed: 2016-04-25).
- [40] S. Garfinkel and H. R. Lipford, "Usable security: History, themes, and challenges," *Synthesis Lectures on Information Security, Privacy, and Trust*, vol. 5, no. 2, pp. 1–124, 2014.
- [41] D. M. Pedersen, "Psychological functions of privacy," *Journal of Environmental Psychology*, vol. 17, no. 2, pp. 147–156, 1997.
- [42] M. T. I. Aumi and S. Kratz, "Airauth: evaluating in-air hand gestures for authentication," in *Proceedings of the 16th international conference on Human-computer interaction with mobile devices & services*. ACM, 2014, pp. 309–318.
- [43] M. Karlesky, E. Melcer, and K. Isbister, "Open sesame: re-envisioning the design of a gesture-based access control system," in *CHI'13 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2013, pp. 1167–1172.
- [44] R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Computing Surveys (CSUR)*, vol. 44, no. 4, p. 19, 2012.
- [45] K. E. Vaniea, E. Rader, and R. Wash, "Betrayed by updates: how negative experiences affect future security," in *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2014, pp. 2671–2674.
- [46] I. Ion, R. Reeder, and S. Consolvo, "... no one can hack my mind: Comparing expert and non-expert security practices," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015, pp. 327–346.

## APPENDIX

### A. Interview script

#### Smartphone usage

- Why did you decide to buy a smartphone?
- You are currently using a smartphone with [Android/ iOS/ windows] operating system (OS). Was this a conscious decision? What were the reasons [for this decision]?
- Have you used another operating system before?
- If so, which? What were the reasons for changing the OS?

#### Smartphone sharing (Adapted from Chin et al. [1])

- Is this your only smartphone?
- If not,
  - How many smartphones do you own?
  - Why do you own several smartphones?
  - Which of them do you use mainly?
- Are there any other people who use your personal smartphone on a regular basis?
  - If so, how many? Who else is using your personal smartphone?
- Is there someone else who sometimes uses your smartphone?
  - If so, under which circumstances?

#### Work related use

- Do you also use your smartphone for work?
- If so,
  - For which purpose [e.g. calling, e-mailing etc.]?
  - What are the main differences between private and occupational use of your smartphone?
  - Did your employer set any requirements for work related smartphone usage?

#### App usage

- Do you use apps?
- If not, why?
- Which are your favourite apps on your smartphone?
- Which apps do you consider the most useful on your smartphone?

### **Paid apps**

- Do you use apps you have to pay for?
- If not, are there any reasons why not?
- If so,
  - How do you pay for the apps?
  - Do you use in-app purchases?
    - \* If so, is the in-app purchase function password protected?

### **App selection and download**

- Which criteria do you use to decide for an app you want to download or install?
- Which platform (i.e. app market) do you use to download apps?

### **App avoidance**

- Are there any apps which you intentionally don't install?  
If so, what kind of apps?

### **App uninstalling**

- Have you ever cancelled the installation of an app? If so, why?
- Have you ever uninstalled an app? If so, why?

### **Smartphone set up**

- When you used your smartphone for the first time
  - How did you take action?
  - Did you set up the device according to your preferences?
  - If so, what did you do?

### **Data connections**

- Which type of data connections do you use (e.g. Bluetooth, NFC, WiFi)? What are you using them for?
- If WiFi was mentioned: Which access points do you use [which networks do you use, respectively]?
- Are there situations in which you switch off your data connections?
- If so,
  - Why?
  - Do you remember any causes that made you start doing so?

### **Updates**

- Do you install app updates?
- If so,
  - Why?
  - Do you install updates automatically or manually?
  - Is there any reason why you install them automatically/ manually?
  - Do you remember any causes that made you start doing so?

### **Post-paid vs. pre-paid**

- Do you pay for your smartphone usage on a monthly basis or do you use pre-paid?

- What are the reasons why you decided for [payment method]?
- If Post-paid:
  - Do you check your monthly phone bills?
  - If so,
    - \* Why?
    - \* Do you remember any causes that made you start doing so?
- If Prepaid:
  - Do you check your prepaid balance from time to time?
  - If so,
    - \* How often?
    - \* Do you remember any causes that made you start doing so?

### **Battery lifetime**

- Do you check your battery status from time to time?
- If so, do you do anything to save battery lifetime?
  - If so,
    - \* Could you please describe what exactly you're doing?
    - \* Do you remember any causes that made you start doing so?

### **Protection from theft**

- Do you do anything to protect your smartphone from theft?
- If so,
  - What are you doing?
  - Do you remember any causes that made you start doing so?
- Do you use locating or remote access apps?
- If so,
  - Why?
  - Do you remember any causes that made you start doing so?

### **Backups**

- Do you make backups of your smartphone data?
- If so,
  - What are the reasons for making backups?
  - How often do you make backups?
  - Where do you store your backups?
  - Do you remember any causes that made you start doing so?

### **Internet und Surfing**

- Do you surf the Internet on your smartphone?
- If not, why not?
- If so
  - Which browser do you use? Why?
  - Which search engine do you use on your smartphone? Why?

- Have you ever changed your browser settings?
  - \* If so, what did you want to change?
  - \* Was the action successful?
- Do you take any measures to reduce your data traces on the web while surfing with your smartphone?
  - \* If so, what do you do?

### Financial Transactions

- Do you use apps which include handling money such as mobile payment, mobile TAN procedures, online banking or shopping apps?
- If not, why not?
- If so,
  - Which kind of apps do you use?
  - Do you have any concerns while using these apps? If so, what kind of concerns?
- Do you use online banking via the browser?
  - If so, how does such a typical banking session look like?

### App access to sensitive data

- Many apps request access to sensitive data (such as calendar or address book) and functions (such as camera and location).
- Do you allow those apps to access this data and functions?
  - If not, why not?
    - \* How do you avoid it?
    - \* Do you remember any causes that made you start doing so?
  - If so,
    - \* Do you allow all apps to access everything or only certain apps?
    - \* Do allow always access or only in certain situations?
  - Do you consider any data or functionalities more sensitive than others?

### Communication

- Do you use your phone to communicate with other people?
- If so,
  - How do you communicate? (e.g. calling, SMS, Chat, email, social networks)
  - Which messaging apps do you use? Why do you use exactly these?
- Do you do something to protect your communication?
- If so, what do you do?
- Whom do you protect your communication from?
- Can you remember any causes that made you start doing so?

### Data stored on the device

- Do you protect the data which is stored on your device?

- If so,
  - How do you protect your data?
  - What do you protect your data from?
  - Do you remember any causes that made you start doing so?

### SPAM

- Do you sometimes receive SPAM (i.e. unwanted adds or messages) on your smartphone?
- If so,
  - Could you give us some examples?
  - How often do you receive SPAM?
  - Do you do anything to reduce the amount of SPAM you receive?

**“Backup” questions:** *Those questions were only asked if the related topics were not already mentioned during the interview.*

- Do you do anything to protect yourself from apps that collect too much data?
- If so,
  - What do you do?
  - How do you define these kinds of apps?
- Do you use additional security software on your smartphone?
- If so,
  - Which kind of apps do you use?
  - Against what do you want to protect yourself?
- Do you use pre-installed security mechanisms such as screen lock with a password?
- If so,
  - What are the reasons therefor?
  - Do you remember any causes that made you start doing so?
- Do you perceive any threats related to smartphone usage?
- If so,
  - Which threats do you perceive?
  - Do you have an individual strategy to protect yourself against these threats?
  - If so, could you please describe your individual strategy?
- Do you perceive any security and privacy threats related to smartphone usage?
- If so,
  - Which threats do you perceive?
  - Do you have an individual strategy to protect yourself against these threats?
    - \* If so, could you please describe your individual strategy?
- Do you have any comments or questions regarding the topics which we discussed today in this interview?

# “It Is a Topic That Confuses Me” – Privacy Perceptions in Usage of Location-Based Applications

Maija E. Poikela, and Felix Kaiser  
Quality and Usability Lab,  
Technische Universität Berlin  
Berlin, Germany  
Email: maija.poikela@qu.tu-berlin.de

**Abstract—** Location-based applications bring ever more possibilities for the users: finding a soulmate, locating good restaurants in vicinity, or tracking a lost phone. Benefits are abundant, but, whether the user realizes it or not, so are the risks. This raises questions about what the users of location-based applications think happens with their location data, whether they see the usage as a tradeoff between benefits and risks, and whether they attempt to protect themselves from privacy risks. We conducted a set of semi-structured interviews (N = 41) with an explorative approach to investigate smartphone users’ perceptions of location-based applications. Among other things, we investigated the benefits that have been experienced, the risks that cause concern, and the expectations of what happens with the location data. The data was then analyzed to further study the relationships between these concepts. Our results suggest that trusting individuals see more benefits in location-based applications than others, and on the other hand, those who express mistrust report more risks than others. Interestingly, participants with some limitations in their knowledge of location-based applications said more often than others that there are no risks in using location-based applications. On the other hand, participants with good knowledge seem to be protecting themselves from privacy risks more.

**Index Terms—**knowledge, location, location-based applications, privacy, trust

## I. INTRODUCTION

IN the age of information technology, the nature of interaction has changed. Unlike in physical world, in online social interactions the audience with whom one interacts is no more physically or temporarily restricted [1]. A comment posted in an online forum today might get a different kind of

interpretation if re-posted and read in a different context, by an audience not originally imagined by the person. This kind of breaking of *privacy boundaries* cause discomfort and privacy issues, since the user is no longer in control of their data [2]. Similarly, when a user’s personal information is used in a context not intended by the individual, boundary turbulence ensues. This applies also for location information.

Location can be considered personally identifiable information, as from one’s movement patterns, a whole range of personal details can be inferred. If location data is also combined with other data such as medical data, or internet searches, a great deal can be inferred about an individual.

To protect oneself from privacy breaches and to be in control of one’s personal information, one should be knowledgeable of what happens with the data. However understanding what happens with one’s data when using online services is non-trivial, and in fact most users have been shown to have no understanding about the data flow, nor about its usage [3]. Privacy policies are lengthy [4], and written in a language incomprehensible to the common user [5].

The number of location-based applications (LBA) has drastically increased within the last decade as smartphones have gained popularity. The location of a device can be calculated using one or several methods, including triangulation based on cell towers, satellites, or Wi-Fi signals. Using more than one of the methods improves the accuracy of the location and overcomes issues in some methods (e.g. the satellite signal getting affected by blocking objects, such as buildings). This information is available for applications installed on the users’ devices and is retrieved either at certain intervals (for example every 5 minutes), or when requested by the user. Location-based applications use this geographical location of a device, providing mobile users a number of functionalities. These include services that use location for finding information such as nearby restaurants, locating one’s lost device, or for social purposes, including finding a partner, or enhancing one’s social status through location check-ins. The location information can also be saved to the user’s profile and the movement traces can be used to provide

Permission to freely reproduce all or part of this paper for noncommercial purposes is granted provided that copies bear this notice and the full citation on the first page. Reproduction for commercial purposes is strictly prohibited without the prior written consent of the Internet Society, the first-named author (for reproduction of an entire paper only), and the author’s employer if the paper was prepared within the scope of employment. EuroUSEC ’16, 18 July 2016, Darmstadt, Germany  
Copyright 2016 Internet Society, ISBN 1-891562-45-2  
<http://dx.doi.org/10.14722/eurousec.2016.23010>

personalized services and offers.

Extensive research has been conducted on the perceived benefits and risks of location-based applications, however, the effect of users' understanding of what happens with their location data on privacy behaviour – on usage of LBA and on protection behaviour – is still lacking. This study aims at extending the knowledge about perceived benefits, risks, and knowledge, with data drawn from users' actual experiences. We also propose a novel taxonomy for the risk-benefit calculation that users engage in when using location-based applications. To achieve this, we conducted a set of semi-structured interviews assessing users' beliefs, and connected their knowledge with stated benefits and concerns. This explorative study suggests that there are a number of misunderstandings regarding location-based applications' data use. We find that the participants with limited knowledge of how location-based applications work – or their data privacy aspects – thought more often than others that there are no risks involved in these applications. Better knowledge, on the other hand, seems to be associated with taking more measures to protect oneself from privacy risks. We also find that users who see the most benefits in LBA were the ones who also stated feelings of trust towards different entities, including companies and governmental organizations. On the other hand, the users who stated comments reflecting mistrust mentioned the most concerns over using of LBA. Among the users, surveillance was mentioned most often as a likely risk.

## II. RELATED WORK

### A. Benefits

The location-based applications offer a wide range of benefits to the users. The biggest benefits of these services that were mentioned in a study by Tsai et al. [6] were security or safety related: finding people in an emergency, or tracking the children in one's family, as well as finding information based on one' location. Tang et al. suggest that most location-sharing is purpose driven rather than social driven, such as arranging meetings or transportation [7]. A variety of social applications have gained huge popularity, including services to find a partner nearby, or informing others about one's whereabouts. Sharing information also helps in promoting oneself and enhancing one's status in social circles. How willing one is to disclose location in various situations is influenced by who the requester of information is [8], [9]. Not only closeness to the receiver of the location information, but also trust in the receiving entity decreases privacy concern [10]. Furthermore, trusting beliefs might, in addition to mitigating concerns of privacy risks, increase the users' willingness to disclose information through location-based services [11].

### B. Concerns

Users have been found to have particular worries when using mobile devices, and mistrust towards smartphone applications creates agitation in users [12]. These worries include physical damage, data loss, battery life, and lack of trust [12]. In another study, the most likely risks the users see

in location-based applications were found to be revealing one's home location, and being stalked (cf. [6]). Also too well targeted advertising seems to create privacy concern and decrease disclosure [13]. Advertising can be seen either as disconcerting or beneficial, depending on the control the user has [14]. The complexity of the topic can be seen in that privacy concern can vary drastically based on the physical situation, or social and technological context [15].

### C. Protecting Privacy

Users have several tools at hand to enhance their privacy when using location-based applications. These include switching the location services off altogether, avoiding the usage of services and installation of applications that require one's location, giving access to location information only to certain people and blacklisting others, or location obfuscation, which refers to giving the user an option to share their location at an accuracy that corresponds to their privacy preferences and use case. Users with higher privacy concern take advantage of this functionality and share with lesser precision [16]. In another study, Consolvo et al. found that users tend to share their private information at an accuracy that is most useful to the user [8]. This functionality is not readily available in most systems to date.

In a study by Toch et al. [17] users were found to evolve more sophisticated privacy preferences over time. In another study, users of location-based applications were also found to have difficulties in expressing their privacy preferences [18].

Privacy breaches may have the consequence for an individual to tighten up their privacy protection mechanisms. This was found in a study with undergraduate Facebook users, where privacy violations led to the users having friends-only profiles [19]. Transparent data privacy practices have also shown to decrease users' privacy concern with respect to surveillance [20]. Not only the data privacy practices of companies behind location-based applications, but also governmental legislations have shown to increase feeling of self-control and decrease concern.

### D. Misunderstandings

A survey from 2003 by Turow et al. revealed that a vast majority of internet users have overly optimistic views of what happens with their data, and at best, a very limited understanding of data privacy practices [3]. Also the users of location-based applications are often unaware of the data that is collected through the apps they use, and informing them prompts to reevaluate some permissions, or even restrict them [21]. The findings by Turow et al. were repeated by Hoofnagle and Urban in 2012 in a study in which participants' knowledge was tested via a quiz about online advertising [22]. The researchers report that users with high privacy concern seem to have a better understanding of information privacy practices than others. In both these studies, the alarming finding is that the users have an unfounded belief that laws and regulations protect their data from being passed on to third parties. Balebako et al. assessed the gap between users' understandings and actual data leakages and found that users

would like to have more information about data sharing than currently available [23]. Many misunderstandings were revealed within the study, including that the users drastically underestimate how much their data is used for different purposes. There is a gap in the literature in to what extent the limited knowledge affects privacy behaviour in the context of location-based applications.

### III. RESEARCH METHOD

To study smartphone users' views and experiences with location-based applications, we conducted a set of interviews. We had an explorative approach, within which we aimed at learning new insights about their experiences and beliefs. The topics covered in the interviews included:

1. Which location-based applications do the participants have? The possibility of some other applications using the location without the users' knowledge was also discussed.
2. Why are the named applications used? What are the benefits the participants see in using location-based applications, and in particular, what kind of benefits have the participants already experienced?
3. What are the reasons for not using some applications?
4. Are the participants aware of any possible risks there might be involved in using location-based applications? Which ones? How did the participants learn about the risks?
5. Has the possible perception of existing risks affected the usage of location-based applications in some way? How exactly?
6. What do the participants believe is done with the users' location information? What do they believe is possible to do with the data? Finally, who is responsible for protecting the user from the possible risks was also discussed with some participants.

Additionally, relationships between the concepts are assessed; we deduct variables from the qualitative interview data to evaluate the relationship of knowledge and privacy behaviour.

#### A. Data Collection

In total 41 semi-structured interviews were conducted during December 2015 (see Appendix A for the basic interview protocol). This method was chosen because of the explorative nature of the goal of the study, and was expected to yield new insights into the users' awareness of location privacy. Most interviews were carried out in a relaxed atmosphere at the participant's home or in a café when the participants were physically available; otherwise they were conducted through a video call. The interviews were conducted in the participants' native languages, with an exception where the participant was fluent in English. All interviews were audio recorded to obtain verbatim statements from all participants; the participants were asked for consent for this prior to the interview. The transcripts were translated

into English prior to analysis by the interviewers, who were fluent both in English and the target language.

#### B. Participants

The participants were voluntary and recruited from the researchers' extended social circles, while aiming at a good demographic distribution. The requirement for participation was smartphone ownership. Of the 41 recruited participants, 14 were female. The age distribution was slightly skewed towards young adults ( $M = 29.6$  years,  $SD = 8.8$ ), which is acceptable considering that among this age group, the users can be considered "smartphone dependent", and the smartphone ownership is highest [24]. Thirty-six percent of the participants were students, and 22% worked in the IT sector. The participants represented 14 different nationalities from five continents; the countries represented in the study were Cameroon (1), China (3), Ecuador (1), Germany (19), Hungary (1), Iran (2), Korea (2), Netherlands (2), Peru (1), Spain (2), Sweden (2), Taiwan (3), UK (1), and USA (1). The participants lived in the mentioned countries, and in the cases where the participants were not physically available for a face-to-face interview, these were conducted via video calls.

### IV. QUALITATIVE FINDINGS

In analyzing the interviews, we used a mixture of inductive and deductive approaches. As a basis for the codebook, we used existing literature, in particular, the expected benefits and risks found in a study by Tsai et al. [6]. Two independent reviewers coded the interviews, with freedom to be open for new codes during the process.

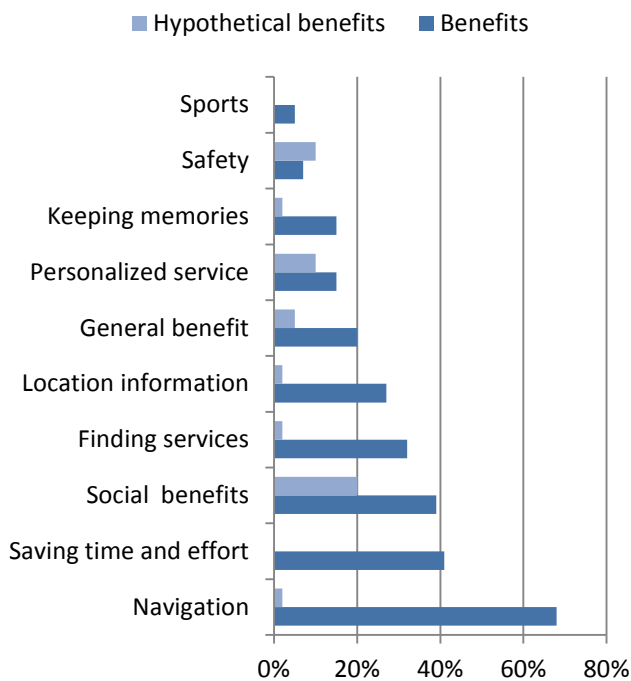
After the first round of coding, the labels were gathered and grouped into meaningful entities. This round yielded to a revised codebook, which was used by the two independent reviewers for a second round of coding. Finally, the remaining disagreements in the labels were resolved and mutual agreements were reached for each case.

In the following section, we explore the qualitative findings from the interviews. We discuss in detail some of the most important emerged topics, together with some examples. Some of the quotations are translations; we strived to stay as true to the original attitude and choice of words as possible.

#### A. Applications

We asked the participants what kind of location-based applications they used on their smartphones. We did not check whether the responses were accurate information but concentrated on the participants' views. Some of the participants, however, checked during the interview which applications they have on their smartphones that use their location. At this point, several participants were surprised about some applications using the device's location without their knowledge, however, in each of the cases plausible explanations were found for why the application in question would need the information.

We found navigation to be the most commonly used application type, with almost all participants using it (90%). This category includes maps, navigation aids, as well as apps



**Fig. 1: Benefits and hypothetical benefits received from location-based applications, ordered based on how frequently each category was mentioned.**

used specifically for public transportation routes and timings.

The second most mentioned app type was social (54%). This included applications where location services were used for social interactions, such as Facebook, WhatsApp, Twitter, Snapchat, Tinder, Instagram, and Skype. Only applications with location functionalities known to the user were considered. However, the location functionalities were not used in all cases.

Twenty-two percent of the participants had applications that they used for finding services, including Yelp, Booking.com, Airbnb, and others. Fifteen percent mentioned using a weather app with location functionality.

The other applications mentioned to be in use were different applications for sport activities (10%), safety applications such as a “find my phone” app (5%), as well as taxi and ride sharing applications (5%). Finally, other location-based applications not included in the above mentioned categories were mentioned by ten participants (24%). These include music streaming, fashion and shopping applications that the participants stated use their location.

### B. Benefits

We asked the participants about the benefits they have experienced with location-based applications. The participants also mentioned benefits that they could imagine existing, or benefits that they believe their friends or family have experienced. We labelled the comments of this latter type as hypothetical benefits to make the distinction between actual benefits and the ones that the participants have not experienced themselves (cf. Fig. 1).

The most commonly stated benefit was, perhaps unsurprisingly so, *navigation* (71%). Forty-two percent of the

participants said that location-based applications have helped them in *saving time and effort*, mostly by simplifying the interaction by requiring less user input. *Social benefits* were also mentioned by 42% of the participants. These included sharing one’s location in a group when setting up meetings, for safety reasons for example in the case of elderly family members or ones with memory issues, location-based gaming, or for social recognition. Social recognition was also mentioned several times, though only as a hypothetical benefit, as stated by participant 18 as follows: “Well, I think this kind of location-sharing app is commonly used by those who want to show off. Those people can share wherever they are [visiting] for example, some fancy, high-class restaurant or going somewhere few people are able to go.” Social benefits were mentioned as a hypothetical benefit by altogether eight participants (20%). The reason for that social recognition was seen only as a hypothetical benefit could be that it might not be socially acceptable to be showing off, and as a consequence, it is safer to avoid talking about it in active voice.

One third of the participants mentioned a benefit of *finding services*, such as stores, restaurants, or accommodation (32%). Other *location Information*, including store opening hours, or information regarding a currently visited point of interest, were mentioned by roughly quarter of the participants (27%). *Personalized service* was mentioned as a benefit by 15 per cent. These included search results that fit to the users’ context, or adverts and promotions based on their location. Four participants thought this could hypothetically be beneficial (10%).

Six participants mentioned *keeping memories* as a benefit (15%). In these cases, location traces would be used mostly as something like diary entries.

A few participants found *safety* features a benefit from LBA (7%). Mentioned benefits were about finding one’s family members or stolen property. Safety was mentioned also as a hypothetical benefit (10%), mainly for being able to track family members who need to be taken care of (such as kids or elderly). Also the possibility for the government to track citizens for safety reasons was brought up.

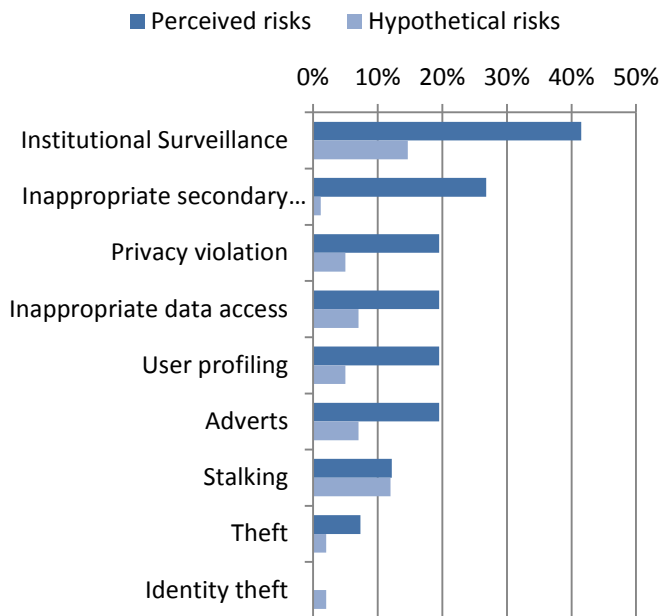
There were two mentions of *sports* as a benefit, including running and biking (5%). Finally, *general benefit* was mentioned by eight participants (20%) including benefits such as convenience, making one’s life better, “connecting the physical world with the virtual world”, or providing a benefit for the society by creating more data.

Also, one tenth of the participants (10%) expresses that the data will be used somehow to develop or improve the services. “For most developers, collecting user information is very important to help improve the quality of service” (P7). This is however not clearly a benefit from using the applications.

### C. Risks and Hypothetical Risks

The participants were asked whether they thought there were some risks involved with using location-based applications. The participants talked mostly about actual risks that one should be aware of, but quite often also hypothetical





**Fig. 2: Risks and hypothetical risks by the number of participants having mentioned them. A risk is called hypothetical if the participant was not currently concerned about it but mentioned it as a hypothetical scenario.**

risks were mentioned. These are risks that are considered possible in some circumstances but are not seen at all likely to happen to oneself, at least with the current status quo. We differentiate between these two by dividing them into separate categories: risks, and hypothetical risks. For an overview, see Fig. 2.

The risk mentioned most often was institutional surveillance – mentioned by 42% of participants. This category includes statements regarding the police or the state following one’s actions. Opinions such as the following were stated: “I’m afraid of the state, institutions, police, that they draw conclusions and predict ‘Minority Report’ style things, and classify you. That’s disgusting, that’s the problem because I think the private sector is not the problem.” (P3), as well as simply: “[...] it’s very easy to spy on people.” (P30) or “There is no better way to control people” (P21). Surveillance was also mentioned by six participants (14.6%) as a hypothetical risk, which means that these people talk about surveillance as a possible risk but do not feel threatened by it, and, more often than not, the possibility leads to no action with respect to privacy behaviour. “If I was on the run and someone with access to the data wanted to find me, then yes, it would be possible to find me. But I’m not on the run since I don’t have any bad things going on” (P27).

The second most reported concern was about *inappropriate secondary use of data* (27%). The participants expressed concern over not knowing what is done with their data, or that it even might be used by people with bad intentions, or sold to third parties without one’s knowledge. The hypothetical risk of inappropriate secondary use of data was expressed by the same concerns, with the difference of not feeling directly threatened by them. “Maybe at this point in time not yet, but in

the future it might be quite dangerous. I mean you never know if someone has a good or bad intention with this data and who they might sell this data to” (P15). Slightly fewer participants reported concern of *inappropriate data access* (20%). While inappropriate data access refers to a situation where the user’s information has gotten in the hands of parties not originally intended, the inappropriate secondary use of data specifies that the information is also used for purposes not originally intended by the data subject, nor permitted by them. A typical comment reflecting inappropriate data access would be, as stated by P15: “Well, the fact that these companies know where you are located and maybe they, I don’t know how it works, but maybe some hackers or someone that’s good with programming can actually also get this information.” Three further participants talked about a hypothetical risk of inappropriate data access.

*Adverts* were worrying eight of the participants (20%), and a connected user worrying also by eight. In some cases the participants combined the concepts; however, mostly what was mentioned was either about adverts or about user profiling. The concepts are closely connected, as adverts here refer to behavioural advertising, which is done based on the user profiles. Altogether either adverts or user profiling was mentioned by 24%.

*Privacy violation* was brought up also by eight participants, possibly in lack of a more precisely directed concern. The statements included comments such as the following: “[...] if talking about the risk, I think it’s about the user’s privacy. For example, I think it’s personal information, it’s private information” (P19).

Stalking was mentioned by five participants as a risk. “[...] you are really transparent, which makes stalking much easier” (P41). In some cases, concern of stalking was seen in hacking, for example, “people could stalk you if they hack the app” (P11). Further five participants saw stalking as a hypothetical risk. Even if the participants are not concerned, they are still aware of the possibility, for example, P27 mentioned the concern as follows: “[...] if my boss could see where I am... Then he could have seen that I’m at a job interview somewhere else. But that takes that there is another person spying on you, otherwise is not a risk. So I don’t really think there are any risks.”

The concern of theft results from the possibility of getting tracked, through self-reports of where you are, for example via social media. “[...] it is a well-known risk that it is not always good to tell everyone where you are all the time. It is not always that good, thefts for example” (P28). Some were also concerned about disclosing home location through tracking: “[...] so he can track where my home is, he can steal my posts” (P1). This category covers two different types of theft: firstly, the risk of thieves getting to know where there is an empty apartment (for example, because of holiday posts on social media), and secondly, of robbery after an individual’s whereabouts have been figured out through the use of location-based applications. Once also a hypothetical risk of theft was mentioned, and it also falls under these categories. Identity theft was mentioned only as a hypothetical risk; it did



not come up as a potential risk that someone would be currently concerned about.

#### D. Trusting Beliefs

*Tradeoff.* Half of the participants felt that there is a tradeoff in using location-based applications (49%). “I take that risk, because I get something instead. But that is the limitation. I need to get something in return, so that I divulge my location.” (P24).

*There is no risk.* Almost half of the participants were of the opinion that there is no risk involved (44%). The vast majority of these stated that only dishonest people have some risks and notably, that “they have nothing to hide”: “Personally I don’t care much. Got nothing to hide. The benefits are more than the inconvenience.” (P8). Others thought that when too much data is being collected, it cannot be used anymore for anything useful – thus there are no risks in data collection.

*Powerlessness.* Many reported powerlessness over their data (42%). These participants are not comfortable about how their data is being handled, or about the lack of control thereof. As an example, P31 commented on the topic of reading app permissions as follows: “[...] the data is stored, but there are so many updates and partially you have to accept various conditions with it, and I don’t know anyone who is reading them carefully and dealing with them. So I think that one quickly loses track of all these functions and updates that you installed on a daily basis, without looking what is now really changed since, I think that is not transparent.”

*Trust.* Trusting comments were stated by every third participant (29%). In many of these comments the participants stated that they trust that companies, in particular big companies such as Google and Facebook, treat their data correctly. “Google is a world-known company, which means they have the obligation to protect the customers’ data. Sometimes those apps asking users’ location only use it for their servers, so no need to worry about that.” (P17). P28 commented on Google: “I don’t think that they would sell the information. That would be bad PR for them.” Several comments also reflected trust in the governmental organizations’ data privacy practices.

*Mistrust.* Comments were labelled as mistrusting when they reflected that the participant did not believe the companies or government organizations are honest about data privacy practices, or when there were feelings that data is being unnecessarily saved or used. These were slightly less common than those stating trust (24%). An example of a statement showing mistrust would be the following by P24: “Well if you hear how all the big companies like Facebook and Google pass information to security agencies... Then I think that they are not able to protect my own privacy.”

#### E. Knowledge

Various comments within the interviews included statements that reflect either misunderstandings of different types with respect to LBA, or a good knowledge of the data flow of LBA or technical understanding of how LBA work.

**Table 1: Protective measures taken against privacy risks on LBA. The categories are partly overlapping, meaning that some participants use more than one protective measure.**

Protective Measures	Percentage
Technical measures	53.7%
Avoiding usage	39.0%
Educating oneself	24.3%
No measures taken	20.0%

The categories are partly overlapping as some participants shared comments showing good knowledge, and on other statements, some misunderstandings. Knowledge was not systematically recorded for all the participants but rather, the issues came up during the interviews. Studying the extent of knowledge of information flows in LBA systematically remains thus a topic for future studies.

*Limited knowledge.* During the interviews, we found a majority of the participants having misconceptions about LBA. Altogether 25 participants (61%) had some limitations in their knowledge. These could be further divided into subcategories:

1. Misunderstanding about some technical detail. The most frequently recorded misunderstanding was that GPS would be the only way of finding out one’s location, and by switching GPS off, the phone’s location could no longer be tracked.

2. Statements where a participant says that they are not fully aware of how things work.

3. Misunderstandings regarding what would be done with the data. For example, some participants were convinced that user profiles are not being used by third parties, or that information is not used because that would be too much effort: “I think they won’t spend so much effort in combining the data?” (P13).

*Good knowledge.* In this category, we included comments that showed good knowledge of how LBA work, for example with respect to what is possible to find out based on the data, or of data protection regulations. “I know that there are certain laws that state how long such information can be saved” (P36).

#### F. Protective Measures

The participants explained what kind of measures they take when they are somehow concerned or see some risks in using location-based applications. The comments regarding protective measures are divided into four categories as follows (c.f. Table 1). The categories are partially overlapping because some participants mentioned more than one such reason.

*Technical measures.* The most popular protective measures category, technical measures, combines all technical possibilities that were mentioned being used to protect oneself, such as switching off location services, or denying location access for some applications. “I turn my location off when I don’t need it” (P9). Others mentioned defining their location settings as a privacy-protection method: “I tick of who is allowed to use it and who isn’t” (P25). The above quotations are typical statements we recorded for protecting measures in

a technical context, mentioned by 54% of the participants.

*Avoiding usage.* 39% of the participants reported avoiding usage, with varying degree of clear privacy reasons. Since we labelled into this category also comments that did not explicitly mention concern, this cannot be taken purely as a measure to protect oneself from privacy concern. A number of privacy-related statements were recorded, including: “[...] when I got the impression that an app which is not at all related to “location”, but is asking for it, then it is enough of a reason for me not to download that app.” (P24). Twenty percent of the participants stated explicitly that they avoid using LBA due to privacy reasons. Other reasons for not using LBA, or avoiding their usage, included not seeing benefits in these applications (37%), annoyance (5%), and technical reasons such as saving battery (10%). These reasons either referred to a single application, or to location-based applications in general. In some cases, participants even stated that they do not have privacy concerns.

*Educating oneself.* Roughly a quarter of the participants expressed statements we covered with the category educating oneself. Exemplary here are comments that one reads the terms of agreement or checks for certain permissions before downloading an application.

*No measures taken.* Finally, one fifth of the participants remarked that they do not take any measures to protect themselves. As an example, participant P3 discussed about data protection and companies knowing where he has been through geotagged pictures as follows: “I feel uncomfortable. I know that, but I kind of ignore it. It is somehow worth it.”

#### G. Source of Information and Responsibility

Some participants reported where they had learned about the data use and risks involved in location-based applications. According to these participants, media was the main source of information, including television, newspaper, radio, and online articles. The information about risks and data misuse comes mostly through reports of scandals. Other mentioned information sources, though playing only a small role, were through work, friends, being self-learned, and other sources.

Some comments were given as to whose responsibility it is to protect the users from privacy breaches. Such comments were recorded only from 27% of the participants. Some users saw that the user is responsible for the data protection. A typical comment stating users’ responsibility was that by P31: “I am responsible for what data I would like to give away, so I can also switch off all the location services and only the network provider knows in which area my phone logs in.”

Even more frequently participants were of the opinion that the state would need to take the responsibility of protecting users. This was stated almost unanimously among the participants who took a stand on whose responsibility data protection is. P32 said: “[...] I don’t really believe that every user has the overview and would be able to protect oneself adequately. I don’t think the App Store as a resell and download platform is the right contact person. Neither are the network providers, because they have nothing to do with the apps. In my opinion the government is responsible for

regulating with laws or at least some rules for the app providers what they are allowed to do and what are not.”

#### H. Other Variables

Here, we present how we deduced variables from the interview data to conduct further analysis.

##### 1) Knowledge

Statements that reflected either good knowledge regarding the functionality of location-based services – or the lack thereof – were partially overlapping. This means that a participant showed good understanding with some comment, and limitations of knowledge could be seen in some other comment by the same participant. We took all comments reflecting either end of this spectrum, and created a new variable called knowledge. This variable measures knowledge on a five-point scale:

1. Limited knowledge (the participant has at least one comment showing limited knowledge, but none showing good knowledge).
2. Both kinds of comments are present, but there are more stating limited than good knowledge.
3. There are as many comments stating good knowledge as limited knowledge, at least one each.
4. Both kinds of comments are present, but more reflect good knowledge than limited knowledge
5. Good knowledge (at least one comment reflecting good knowledge and none of limited knowledge).

On this new scale, mean was 2.85, and standard deviation 1.67. Seventeen percent of the participants were not categorized because of lack of comments that could be used to categorize them, thus, they are excluded from the analysis related with knowledge. Some of the limitations are more severe than others and thus have unequally big consequences on privacy behaviour; the same applies also for good knowledge. Taking these differences into account is out of the scope of this work and a topic for future research.

##### 2) Benefits and Risks

We created a variable listing the number of different types of benefits that were seen in using LBA to quantify the perceived usefulness of LBA. The median number of benefits mentioned was two ( $M = 2.73$ ,  $SD = 1.57$ ). Similarly, we counted the amount of different risks that are seen in using LBA and introduced a variable that lists the sum. Also for this variable the median was two ( $M = 1.63$ ,  $SD = 1.55$ ).

We created six binary variables of whether or not the most commonly mentioned risks were mentioned by the participant. We considered only the actual risks, and not the hypothetically mentioned ones. The considered risks were *surveillance*, *secondary use of data*, *privacy violation*, *inappropriate data access*, *user profiling*, and *adverts*.

##### 3) Trust

We created a variable to measure trust similarly as to measure knowledge (cf. Section IV.H.1). On this five-point scale (‘1’ representing most mistrusting, and ‘5’ representing most trusting) the mean trust score was 3.21 ( $SD = 1.90$ ). Altogether 46.3% of the participants (19 individuals) were

given a trust score; others did not state comments that could be regarded either as trusting or mistrusting. While it could be argued whether trust can be considered a trait, we consider the participants who stated mostly trusting comments as *trusting individuals*, whereas the participants whose comments reflected mostly mistrust, we call *mistrusting individuals*.

## V. RESULTS

In an attempt to find out about the relationships between the various concepts found in the data, we ran tests using the statistical tool SPSS. Our goal was to gain some insight to how knowledge and beliefs affect users' privacy behaviour. As our variables were not systematically measured from all participants, these results should be taken rather as directive, than conclusive. While we cannot state anything about causality, we did find some relationships between these concepts.

### A. Knowledge

We looked at the association between knowledge and taking protective measures against privacy risks. A Mann-Whitney U-test showed that the participants who stated avoiding usage of location-based applications have a significantly higher knowledge score than those who do not ( $U = 84.0, p = .043$ ). Furthermore, statements implying that there are no risks involved were stated significantly more frequently by participants with lower knowledge scores ( $U = 66.5, p = .006$ ).

We also found that the users who felt that there was no risk to their privacy associated with using location-based applications did not take technical measures to protect themselves,  $\chi^2(1, N = 41) = 5.33, p = .023$ .

### B. Trust and Mistrust

A nonparametric correlation test showed a moderate positive correlation between trust and the number of benefits seen ( $r_s(17) = .449, p = .027$ ). On the other hand, a moderate negative correlation was found between mistrust and the number of risks seen ( $r_s(17) = -.395, p = .0479$ ).

The users who take technical measures to protect their privacy when using location-based applications are significantly more mistrusting than those who do not,  $U = 18.00, p = .027$ . Similar effects were not found with educating oneself, nor with avoiding usage.

Some participants stated that it is a tradeoff to use location-based services – mostly a tradeoff between receiving benefits and losing privacy. The participants who talked about a tradeoff were more concerned about surveillance than others,  $\chi^2(1, N = 41) = 4.19, p = .042$ .

## VI. TAXONOMY

Assuming that a user of location-based services engages in a cost-benefit calculation to define whether or not the benefits of using a given service outweigh the possible risks, we propose a first step towards a taxonomy of cost-benefit calculation in the usage of location-based applications (cf. Fig. 3). The calculation consists of perceived risks and perceived benefits. Different categories are expected to have different

weights in the calculation. The categories were validated in a small user study with participants who were not familiar with this study ( $N = 8$ ).

Within the perceived benefits, five categories were identified: saving time and effort, social benefits, safety, finding information, personalized services, and quantified self. Monetary benefit was not mentioned in the interviews, and its inclusion in the taxonomy is a topic for future research.

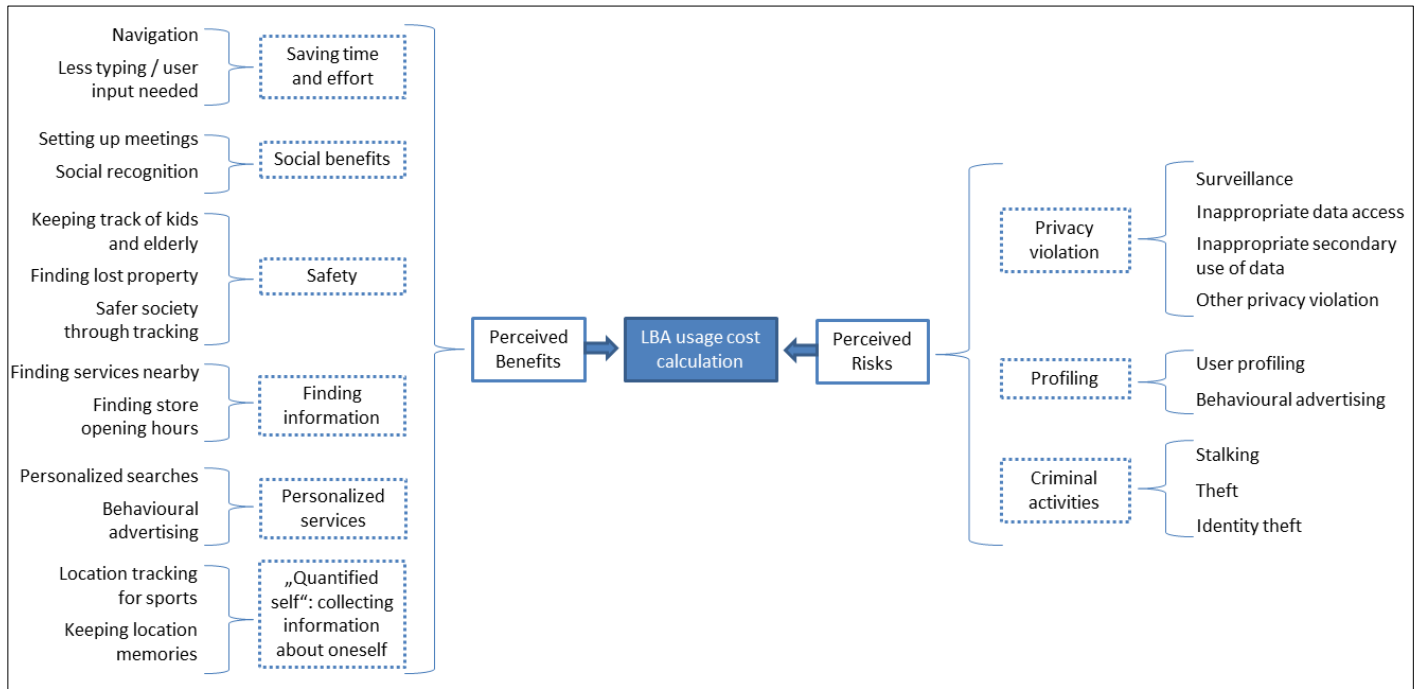
The perceived risks can be further divided into related categories – three such categories were identified. These include surveillance, privacy violation, profiling, and criminal activities. Privacy violation includes surveillance, inappropriate data access and inappropriate secondary use of data, as well as other cases where the user feels that their privacy has been violated. Inappropriate data access is an inevitable first step before inappropriate secondary use of data, however is not necessarily followed by it. Profiling consists of user profiling, and the related behavioural advertising. Behavioural advertising was identified also as a benefit based on the interview data, and is the only item that is found on both the sides of the calculation. Finally, criminal activities include stalking, theft, and identity theft.

## VII. DISCUSSION

In this work we conducted qualitative interviews on the usage of location-based applications (LBA), and propose a taxonomy based on the findings. The taxonomy considers the found perceived benefits and perceived risks as input parameters for a cost-benefit calculation when users make a privacy decision of whether or not to engage in the usage of such an application. The other findings from the study are discussed here.

### A. Misunderstandings

There were several misunderstandings found about how LBA work. The most common misunderstanding was that by switching the GPS off, one's location could not be tracked anymore. The participants with less knowledge also turned out not to protect themselves from privacy risks by avoiding usage of LBA as much as those who did not have such limitations in their knowledge. It seems plausible that users with such limitations did not think there is privacy risks involved in using LBA, and as a consequence, did not see any reason to avoid using them. The connection could be also seen in that users, who said that there are no risks involved, also did not use technical measures, such as switching the location services off or uninstalling applications, as often as others. Location blurring was not mentioned by any participants as a protection method – perhaps the option is still not that readily available. Some individuals stated privacy concern and also admitted that their knowledge is still limited. Nowadays, having some basic understanding of the information flow, or at least of the possible risks, is a precondition to being in control of one's personal information. The results of this study suggest that the user should have less responsibility and be adequately protected even without extensive knowledge about data privacy issues.



**Fig. 3: Proposed taxonomy for cost-benefit calculation in the context of usage of location-based applications. The calculation is done based on perceived benefits and perceived risks. The first can be divided into five, and the latter into four categories.**

A majority of the participants who said that there is no risk also said that they “have nothing to hide”. This statement has been discussed in recent literature: Solove discussed the concept stating that often the users who say they have nothing to hide have a very myopic view of what “privacy” means, understanding it merely as secrecy – hiding something bad [25]. Also our study supports the assumption that the “nothing to hide” view could be a consequence of a myopic view and limited knowledge. Our results show that there is a difference between the knowledge scores of the users who state that there are no risks involved in using LBA: the users who think there are no risks have a significantly lower knowledge score than those that do not. We also find that the users who avoid using location-based applications, for privacy reasons or otherwise, have higher knowledge scores than others. It could be that the users with better knowledge are more aware that there might be some risks involved, and as a consequence they avoid using location-based apps, or use technical measures. This is, however, a speculation and cannot be directly inferred from the data. The interpretation is nevertheless in line with an earlier finding that the internet users who can be categorized as privacy fundamentalists based on the Westin categorization [26] also have a better understanding of what happens with the data [22]. However, it has been suggested that other instruments might provide better options than this categorization [27].

### B. Perceived Risks

In an earlier study, the most salient risks in using LBA were reported to be revealing one’s home location, and getting stalked [6]. These particular concerns came up also in our study, but these were some of the least mentioned ones. The most frequently mentioned risks in this study were

surveillance and secondary use of data. Also rather often mentioned issues were a general privacy violation, inappropriate data access, user profiling, and adverts.

We would also like to point out two distinctive cases of perceived risks – the risk of location information being inappropriately accessed or used by individuals, or by companies and institutions. The concerns categorized as surveillance or profiling include a worry of the data being accessed by organizations, whereas statements categorized as privacy violation and criminal activities reflect worries that the information is finally used by unauthorized individuals.

### C. What Is Done With Location Information?

What do users think happens with the data when they use LBA? Majority of the participants stated that it is used for user profiling, and half mentioned that it is sold to third parties. This is not to say that the rest of the participants did not think that profiles are created or data is sold – they just did not mention it within the interviews. These results also do not take a stand on whether the participants thought the practices are beneficial or harmful.

### D. Protective Measures and Avoiding Usage

The most important reason for not using LBA was stated as not seeing benefits in the usage. Privacy concern seemed to also be an important reason for many; approximately one fifth of the participants stated privacy issues as the reason for not using LBA. It seems that more often than avoiding usage to protect themselves from privacy risks, the users take some technical measures. This includes turning the location service off, or even uninstalling applications. This was particularly typical for users showing mistrust towards different organizations, including governmental organizations and companies. Privacy measures such as blacklisting people, or

location obfuscation, were not mentioned by our interview participants. It can be that these options are not readily available in most applications that the participants use. Avoiding usage of particular applications, or location-based applications altogether, was mentioned by nearly 40% of the participants; however, not all of these are necessarily for purely privacy reasons.

While an important reason for not using location-based applications is not getting benefits out of the usage, many of those who still continue using the LBA find that there is a tradeoff, and one has to compromise privacy to get a benefit. The feelings of tradeoff were in particular associated with concerns of surveillance. Often also powerlessness over one's data was expressed. Both these statements suggest that there is not enough transparency, and users do not know whom to trust.

#### E. Who Protects?

Whose responsibility is it finally to care for end-user privacy? This topic has been previously discussed by Cottrill with a review of legal, technological, and practical aspects of protection [28]. In our study the topic was not discussed by all the participants, however, nearly all of these stated that it is indeed the state's responsibility. In this study we heard also several comments of mistrust towards data protection laws, and in particular, towards the potential big brother effects that could ensue. In earlier studies, government regulations have shown to increase trust [29] – but the condition for this might be an adequate base level of trust towards the governmental data privacy practices.

### VIII. CONCLUSIONS

Our most important results are qualitative findings from 41 interviews conducted with participants from various countries. Our results suggest that a large number of users of location-based applications have overly optimistic views about what is done with the users' data, and that the limitations on knowledge are often associated with statements that no risks are included in using location-based applications. The lacking risk perception could be an explanation to why users with limited knowledge were also found to take fewer measures to protect themselves from privacy risks when using these applications. We also find a sizable user segment that is mistrusting towards companies and governmental organizations, which is associated with seeing more risks in using location-based applications and with using protection mechanisms against privacy risks. We also identified a prominent feeling of a tradeoff accompanied with using location-based applications – the users think there are risks, but accept them as a price they have to pay when using these services. Our findings suggest that in particular, for the user segment with limited knowledge, an adequate level of privacy protection should be provided also without explicit user action.

### IX. REFERENCES

[1] L. Palen and P. Dourish, "Unpacking 'privacy' for a networked

world," *Proc. Conf. Hum. factors Comput. Syst. - CHI '03*, no. 5, p. 129, 2003.

[2] S. Petronio and W. T. Durham, "Communication privacy management theory," *Engaging theories in interpersonal communication: Multiple perspectives*, 2008.

[3] J. Turow, L. Feldman, and K. Meltzer, "Open to Exploitation: America's Shoppers Online and Offline," *Annenb. Public Policy Cent.*, p. 10, 2005.

[4] A. McDonald and L. F. Cranor, "The Cost of Reading Privacy Policies," *I/S - A J. Law Policy Inf. Soc.*, vol. 4, no. 3, pp. 1–22, 2008.

[5] C. Jensen and C. Potts, "Privacy policies as decision-making tools," *Proc. 2004 Conf. Hum. factors Comput. Syst. - CHI '04*, vol. 6, no. 1, pp. 471–478, 2004.

[6] J. Y. Tsai, P. G. Kelley, L. F. Cranor, and N. Sadeh, "Location-Sharing Technologies: Privacy Risks and Controls," *A J. Law Policy Inf. Soc.*, vol. 6, no. 2, pp. 119–151, 2010.

[7] K. Tang, J. Lin, and J. Hong, "Rethinking location sharing: exploring the implications of social-driven vs. purpose-driven location sharing," *Proc. 12th ACM Int. Conf. Ubiquitous Comput. - Ubicomp '10*, vol. 12, no. 4–5, pp. 85–94, 2010.

[8] S. Consolvo, I. E. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge, "Location disclosure to social relations," in *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '05*, 2005, p. 81.

[9] J. Venkatanathan, J. Lin, M. Benisch, D. Ferreira, E. Karapanos, V. Kostakos, N. Sadeh, and E. Toch, "Who, when, where: Obfuscation preferences in location-sharing applications," *ISR Technical Reports 2011, CMU-ISR-11-110, Carnegie Mellon University*. pp. 1–12, 2011.

[10] H. J. Smith, T. Dinev, and H. Xu, "Theory and Review Information Privacy Research: an Interdisciplinary Review 1," *MIS Quarterly/Information Priv. Res.*, vol. 35, no. 4, pp. 989–1015, 2011.

[11] H. Xu, H. Teo, and B. C. Y. Tan, "Predicting the adoption of location-based services: the role of trust and perceived privacy risk," *Proc. 26th Int. Conf. Inf. Syst. (ICIS 2005), Las Vegas*, no. Beinat 2001, pp. 897–910, 2005.

[12] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, "Measuring user confidence in smartphone security and privacy," *Proc. Eighth Symp. Usable Priv. Secur. - SOUPS '12*, no. 1, p. 1, 2012.

[13] A. Goldfarb and C. Tucker, "Online Display Advertising: Targeting and Obtrusiveness," *Mark. Sci.*, vol. 30, no. 3, pp. 413–415, 2011.

[14] M. Benisch, P. G. Kelley, N. Sadeh, and L. F. Cranor, "Capturing location-privacy preferences: Quantifying accuracy and user-burden tradeoffs," *Pers. Ubiquitous Comput.*, vol. 15, no. 7, pp. 679–694, 2011.

[15] L. K. John, A. Acquisti, and G. Loewenstein, "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information," *J. Consum. Res.*, vol. 37, no. 5, pp. 858–873, 2011.

[16] M. Poikela, R. Schmidt, I. Wechsung, and S. Möller, "Locate!-When do Users Disclose Location?," in *Workshop on Privacy Personas and Segmentation (PPS) at the Tenth Symposium On Usable Privacy and Security (SOUPS)*, 2014.

[17] E. Toch, J. Cranshaw, P. H. Drielsma, J. Y. Tsai, P. G. Kelley, J. Springfield, L. Cranor, J. Hong, and N. Sadeh, "Empirical models of privacy in location sharing," *Proc. 12th ACM Int. Conf. Ubiquitous Comput. - Ubicomp '10*, p. 129, 2010.

[18] N. Sadeh, J. Hong, L. Cranor, I. Fette, P. Kelley, M. Prabaker, and J. Rao, "Understanding and capturing people's privacy policies in a mobile social networking application," in *Personal and Ubiquitous Computing*, 2009, vol. 13, no. 6, pp. 401–412.

[19] F. Stutzman and J. Kramer-Duffield, "Friends only: Examining a privacy-enhancing behavior in Facebook," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2010, pp. 1553–1562.

[20] A. Oulasvirta, T. Suomalainen, J. Hamari, A. Lampinen, and K. Karvonen, "Transparency of intentions decreases privacy concerns in ubiquitous surveillance," *Cyberpsychology, Behav. Soc. Netw.*, vol. 17, no. 10, pp. 633–638, 2014.

[21] H. Almuhammedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L. Cranor, and Y. Agarwal, "Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging," *Proc. 2015 ACM Conf. Hum. factors Comput. Syst.*, pp. 787–796, 2015.

[22] C. J. Hoofnagel and J. M. Urban, "Alan Westin's Privacy Homo

- Economicus,” *Wake Forest Law Rev.*, vol. 49, no. 2, pp. 261–317, 2014.
- [23] R. Balebako, J. Jung, W. Lu, L. F. Cranor, and C. Nguyen, “‘Little Brothers Watching You’: Raising Awareness of Data Leaks on Smartphones,” *SOUPS '13 Proc. Ninth Symp. Usable Priv. Secur.*, pp. 12:1–12:11, 2013.
- [24] A. Smith, K. McGeeney, L. Rainie, and S. Keeter, “U.S. Smartphone Use in 2015,” *Smartphone Differ.*, p. 60, 2015.
- [25] D. J. Solove, “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy,” *San Diego Law Rev.*, vol. 44, pp. 1–23, 2007.
- [26] P. Kumaraguru and L. Cranor, “Privacy indexes: A survey of westin’s studies,” *Science (80-. )*, vol. Tech. rep., no. December, pp. 1–22, 2005.
- [27] S. Preibusch, “Guide to measuring privacy concern: Review of survey and observational instruments,” *Int. J. Hum. Comput. Stud.*, vol. 71, no. 12, pp. 1133–1143, 2013.
- [28] C. D. Cottrill, “Location privacy: Who protects?,” *URISA Journal-Urban Reg. Information Systems Assoc.*, vol. 2, no. 23, p. 49, 2011.
- [29] C. W. Thomas, “Maintaining and Restoring Public Trust in Government Agencies and their Employees,” *Adm. Soc.*, vol. 30, no. 2, pp. 166–193, 1998.

## Appendix

### A.1 Interview Script

- How many location-sharing applications do you have on your smartphone?
    - Which ones?
  - Which other applications do you have?
    - Are there some applications that potentially use location features without your knowledge?
  - Why are the mentioned location-based applications being used?
  - If you do not use location-based applications, why not?
- What are some possible benefits you think there are in using location-based applications?
  - What kind of benefits have you already had?
  - Have you heard of any possible risks that there might be?
    - What risks?
    - How have you heard about the risks?
  - How has the knowledge of possible risks affected the use of location-based applications?
    - Have you chosen not to install some applications?
    - Have you used applications less or differently because of the knowledge?
  - What do you think is done with your data?
  - Do you believe the companies that create location-based applications can access your location data?
  - What do you believe the companies do with the location data?
  - What do you believe is possible to do with the location data?
  - How likely do you believe it might be that...
    - ...your home or work address becomes known?
    - ...the data is collected to be sold to third parties such as advertisers?
    - ...the data is collected to create a profile of you?
    - ...the data is combined with other information to create a profile of the user? ...and sold to advertisers?

# Why Do People Adopt, or Reject, Smartphone Password Managers?

Nora Alkaldi & Karen Renaud

School of Computing Science

University of Glasgow

Email: n.alkaldi.1@research.gla.ac.uk; karen.renaud@glasgow.ac.uk

**Abstract**—People use weak passwords for a variety of reasons, the most prescient of these being memory load and inconvenience. The motivation to choose weak passwords is even more compelling on Smartphones because entering complex passwords is particularly time consuming and arduous on small devices. Many of the memory- and inconvenience-related issues can be ameliorated by using a password manager app. Such an app can generate, remember and automatically supply passwords to websites and other apps on the phone. Given this potential, it is unfortunate that these applications have not enjoyed widespread adoption. We carried out a study to find out why this was so, to investigate factors that impeded or encouraged password manager adoption. We found that a number of factors mediated during all three phases of adoption: searching, deciding and trialling. The study’s findings will help us to market these tools more effectively in order to encourage future adoption of password managers.

**Index Terms**—Password managers, Adoption factors, Smartphone applications, Password security

## I. INTRODUCTION

Passwords constitute a crucial barrier to repel attackers. The barrier is weaker than it could be because users choose weak passwords, and those who do choose strong passwords are likely to write them down, which defeats the purpose of a secret authenticator [1, 2]. Many of these coping behaviours occur because users have difficulty remembering all their passwords. Smartphone password management adds another dimension to this, with limited screen size and keyboard multi-layer interaction making password entry arduous [3].

Password managers remove the effort from password management. These applications act as a vault for all of a person’s passwords, with access controlled via one master password. The person only has to remember one password rather than tens of passwords, so memory load is drastically reduced. Password managers also auto-fill credentials, rendering shoulder surfing futile [4]. The resulting strength makes brute force and dictionary attacks less likely to succeed [5]. Despite these

obvious benefits very few people use password managers. One study on 836 employees in a large organisation reported that only 1% used password managers [2].

This poor adoption applies to many security tools [6][7], [8], not only password managers. Poor usability has often been blamed for non-adoption of security measures [9, 1]. However, even usable techniques, such as biometric authentication, have not enjoyed widespread adoption [10]. A survey of iPhone users in Saudi Arabia [11] found that even though the majority of respondents agreed that TouchID was usable and secure, only 33% actually used it for securing their devices.

Much of the research literature focuses on the technical and design aspects of these tools, either attempting to improve usability, security, or both. To the best of our knowledge, only one study by Chiasson *et al.* in 2006 [12] considered the user’s perspective. They detected usability issues, but did not really examine adoption factors. Further investigation is needed to understand why people do, or do not, use password managers.

In this paper we report on an investigation into the following:

- Current usage of password managers (in 2016).
- An investigation into factors impacting on the adoption, or rejection, of Smartphone password managers.

## II. RELATED WORK

Prata *et al.* [13] suggest that people go through three phases with respect to mobile phone apps: *Search*, *Purchase* and *Evaluate*. Häubl and Trifts [14] also refer to these three activities but do not incorporate them into a life cycle model. We depict the adoption phases in Figure 1, renaming “purchase” to “decide”, since many of these apps are free. The figure shows how different factors feed into the phases.

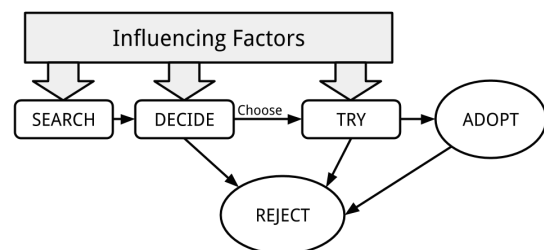


Fig. 1. Smartphone application adoption life cycle

Permission to freely reproduce all or part of this paper for noncommercial purposes is granted provided that copies bear this notice and the full citation on the first page. Reproduction for commercial purposes is strictly prohibited without the prior written consent of the Internet Society, the first-named author (for reproduction of an entire paper only), and the author’s employer if the paper was prepared within the scope of employment.

EuroUSEC ’16, 18 July 2016, Darmstadt, Germany  
Copyright 2016 Internet Society, ISBN 1-891562-45-2  
<http://dx.doi.org/10.14722/eurousec.2016.23011>



The **search** phase occurs when someone becomes aware of the existence of these applications. After the user initiates a search, a number of applications will be presented. The **decide** phase incorporates the decision to install one of the applications or to reject the idea. In the case of choosing to install one of these applications, the user moves to the third phase of the application life cycle where he or she **tries** the application and decides either to continue using it or to discard it. The arrow from Adopt to Reject was added based on arguments by Böhmer *et al.* [15], who talks about mobile app usage, describing the “try” phase, where an initial period of adoption can be followed by rejection, or adoption and continued use.

### Tool Adoption Factors

1) *General Adoption Factors*: Nikou [16] systematically reviews the adoption literature and highlights three meta-categories of factors: **contextual, psychological & social** and **age-specific** factors. The first group includes *cost, perceived usefulness* and *context of use*. The second includes *social aspects* and *barriers to use*, while the third includes aspects such as *technology anxiety* and *resistance to change*. He emphasises the importance of the sociological & psychological factors in predicting adoption.

Hassan *et al.* [17] investigated the determinants behind Smartphone users’ intention to adopt applications with students in Pakistan. They report on mostly contextual factors such as *perceived usefulness* and *perceived ease of use* but also refer to *social need* as an influential factor. These factors are confirmed by [18].

Another contextual factor was reported by Chong [19], who found that *cost* was a significant factor influencing the adoption of m-commerce. This finding was confirmed by [20]. Kit [21] identifies a number of pertinent contextual adoption factors: *performance expectations* and *effort expectancy*. The latter is confirmed by [22].

Another meta-category that emerges from the literature is that of *hedonic* factors [15]. Hassan *et al.*’s [17] study do not report on perceived enjoyment but Yang [18] confirms enjoyment as an adoption factor, as does Kit [21].

2) *Specific App Adoption Factors*: Some researchers have studied specific app adoption, such as the ‘Snapchat’ messaging application [23, 24, 25]. Vaterlaus *et al.* [23] studied Snapchat application usage by young adult Smartphone owners and found that it impacts their interpersonal relationships with friends and family. This adoption factor is confirmed by [26].

Cho *et al.* [27] developed a theoretical model of the adoption of health-related mobile applications. They reported that *consciousness, health information orientation, eHealth literacy, Internet health information use efficacy* and *subjective norms* all play a significant role in influencing the intention to use health applications. Some of these are clearly specific to health-related apps, and might not apply to security app adoption but subjective norms and efficacy (perceived usefulness) can be expected to influence adoption of other apps as well.

Some researchers focused on the impact of adoption factors related to biometric authentication on mobile phones. The impacting factors for these mechanisms are related to *ethical & social* concerns, probably due to the inherently personal nature of biometrics [28].

Sandholzer *et al.* [29] investigated adoption of educational Smartphone apps. They found that gender, interest in new technologies and perceived benefit (perceived usefulness) impacted adoption. Moreover, they also report that previous experiences of educational app usage predicted adoption. Kit [21] also found that previous usage (habit) influenced future adoption.

3) *Summary*: To summarise, the adoption factors that have been identified by other researchers are:

**Contextual**: perceived usefulness [21, 17, 27], perceived ease of use [17, 27], security [30], cost [19, 20], required effort [21], gender and interest in new technologies [29].

**Psychological & Sociological**: core features supporting relatedness/social need [23, 17, 25], subjective norms [27], ethics [28], habit [21].

**Age-Specific**: Technology anxiety, resistance to change [16].

**Hedonic**: enjoyment [21].

Few of these have been tested in the context of security tools, the focus of this paper. We will return to this list once we have presented our findings in order to consider which of these were confirmed, or not confirmed, by our study.

### Smartphone Password Manager Applications

A number of password managers are available for mobile platforms. These applications differ in terms of features and functions that are offered to meet users’ needs (see Table II in the Appendix)<sup>1</sup>. If one examines the table, we see that some of the applications store passwords in local storage (1Password); others rely on cloud services for storage and synchronisation (LastPass). Others use a hybrid approach which stores passwords both locally and on the cloud. Many of these applications require a strong master key (Dashlane); others have no restrictions on the chosen key so as to minimise forgetting (1Password). To support the memorability of the master key, some offer a ‘hint’ feature either shown on the login screen or sent to the registered email address. Some of these applications have started to utilise the presence of the ‘fingerprint’ feature on recent Smartphone devices as an alternative authentication mechanism. Based on this review it is clear that the poor uptake of these tools is not due to a lack of choice.

## III. METHODOLOGY

Two types of data were collected:

- 1) reviews from application stores representing the opinions of users who chose to trial password managers;

<sup>1</sup>These examples have been selected based on their popularity in the iPhone App and/or the Google Play store. The cost and storage requirements were considered to cover a variety of features. The information was gathered in Nov 2015 and kept current by incorporating later reviews.



- 2) an online survey gathering 352 responses about password manager use, and exploring factors that encourage or discourage password manager adoption.

#### A. Reviews

As a preliminary investigation to help us understand why users use Smartphone password managers we analysed users' reviews of the two most popular password manager applications, namely LastPass and 1Password, on Google's Play store [31], and the Apple store [32] in three countries: UK, US and Saudi Arabia. The choice of three different countries was to include different populations of users to uncover region-specific usage patterns, and these three countries were chosen to reflect countries at different stages of technological development. A similar approach was used by [33] and [34] to reveal users' perceptions of applications in Google play and Apple stores. The idea was to use the most recent 20 reviews for each of the two password managers in each of the two stores. Reviews in Google play can be sorted by date, helpfulness or rate. It is recommended to have a minimum sample size of 20 for each culture measure in [35]. Surprisingly, in the Saudi Arabian store, no reviews or ratings were found for either application<sup>2</sup>. Although this does not mean that these applications are not used in Saudi Arabia, it might suggest they do not as readily review applications. It also gives an initial indication of the popularity of password managers as compared to other types of applications such as messaging apps. The latter are highly rated in Saudi Arabian App store. In the end, 120 user reviews were analysed to identify adoption factors. Among them, there were 60% positive reviews. A review was considered positive if it contained more positive than negative sentences. The sentence is rated as positive if it contains positives terms to indicate satisfaction.

#### B. On-line survey

An open-ended questionnaire was designed and validated by testing it with 34 randomly selected testers. Ethical approval was granted by the College of Science and Engineering at the University of Glasgow. It was posted in April 2016 via Google Survey. Using an online survey allowed us to elicit responses from Smartphone users worldwide and the afforded anonymity to offset social desirability bias [36]. Participants were recruited using a snowball sampling methodology, via email and social media such as WhatsApp, Facebook, Twitter and Path. To avoid incomplete participation due to fatigue, a maximum of five questions were posed. To encourage disclosure we did not collect any identifying information or demographics. We received 370 responses; 3 were incomplete, 4 skipped 1 question and 11 were either invalid or the respondents clearly did not engage with the survey. After excluding these responses we were left with 352 usable responses.

<sup>2</sup>This is also true in almost all app stores in other Arabic countries: UAE, Qatar, Bahrain, Oman and Egypt

## IV. RESULTS

A thematic analysis was conducted by two analysts (the authors). High level themes were established based on the analysts' individual reading of the collected data. The data were then coded according to the themes. A second analysis was carried out on the resulting categories aiming to explore sub-themes. The second analysis was done by one analyst and reviewed in detail by the other; an approach deemed sufficient giving that this is an exploring study.

After analysing the results of the survey and the reviews, some adoption- and rejection-related factors emerged which fell naturally into the three Smartphone Application Life Cycle phases, as shown in Figure 2.

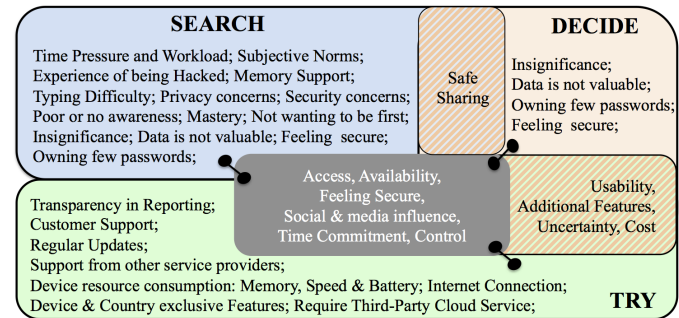


Fig. 2. Search, Decide and Try Factors

#### A. Password Manager Usage

Based on the online survey, we investigated the widespread of password manager usage. Although this was self-reported, 62 respondents (17.6%) said that they used a password manager application on their phone. However, only 24 of them (6.8%) provided the name of a secure password manager application; the rest either misunderstood the question or used other methods that they thought were password managers. Thirteen used PC-based password managers. About half of the Smartphone password manager users (32) misunderstood the term 'password manager application' (even though a brief description of these tools was provided at the beginning of the questionnaire). Some thought it was the screen lock mechanism. Two respondents considered their mailbox and notepad a tool for managing passwords. Four users stated that they used the Google Chrome password manager. While Google Chrome can overcome the password memorability issue, it constitutes a huge threat due to the fact that such passwords are easily accessed in the clear. The use of this memory aid might prevent adoption of a secure password manager. Usage was low: somewhat higher than that reported by Hoonakker [2] but, given the fact that almost a decade has passed, the increase is paltry.

#### B. Factors Leading to Adoption

Based on the analysis of the reviews and responses from the survey, some factors that influence users' decisions to start using password managers, or to continue using them in the

long term, have been identified. Where the theme confirms a theme suggested by the literature this is shown in brackets.

### **Subjective norms**

One of the reviews emphasised the role of subjective norms i.e. the perceived social pressure to engage, or not to engage, in a certain behaviour. In terms of influencing people to use password manager applications:

*“In fact, it’s not just about you, but about your family, friends, and colleagues. Have you considered that when your computer, mobile device, or online accounts are stolen or hacked that you may be exposing information about your family members, friends, and colleagues? Well, the truth is, you are (Review)”*

### **Time (Perceived Usefulness)**

Password managers saved people time that had previously been spent on logging in manually:

*“go read a book or something with all the free time you now have.(Review) ”*

### **Work Demands (Perceived Usefulness)**

In some reviews, users stated their need to accomplish their work on time that requires them to deal with many passwords, and they found it helpful to use such applications. For example:

*“Being an IT/Network Administrator, and having to remember over a 100 different logins and passwords, this thing is a life saver (Review)”*

*“this app has been essential for my day to day work with my 130 something logins (Review)”*

*“If you’re like me, then you have 50+ login credentials throughout the Internet (Review)”*

*“It has truly kept me from losing my mind due to the amount of passwords stored in my head (Review)”*

### **Experience of Being Hacked (Experience)**

A couple of reviewers stated that their experience of previous attack influenced them to start using password manager applications:

*“the headache that comes with it, as happened to me after my email address and password were kindly hacked into by someone in China and displayed online along with the other 300 000. I only found out by curiosity in searching for my email address.(Review)”*

*“It was literally just by sheer luck that I captured it before it happened. I used similar passwords for almost everything and let a colleague type in my password on my office PC while I was in the middle of something else. Big mistake. He “jokingly” logged onto my Twitter and Facebook accounts and put up comments without my knowledge. Although it was a joke to him and I wasn’t upset, it made me think, so the following day I downloaded LastPass and changed all my passwords to 256 bit AES encryption.(Review)”*

### **Memory Support (Perceived Usefulness)**

One of the strongest reasons for adopting these tools, according to both survey respondents and reviewers, is the

memorability issue. The fact that many users possess increasing numbers of accounts makes it a challenge for most of them to construct unique and secure passwords that they can remember. This encourages the adoption of password manager applications. Here are some examples of 5-star rated reviews:

*“For me, it’s a great tool not having to remember numerous login details...(Review)”*

*“I was struggling to remember all the different passwords I had at all the different websites I visited (Review)”*

*“I used to have a single password for all of my secure sites due to the hassle of trying to remember multiple ones. Then I discovered Lastpass. This makes logging in to all of your secure pages simple and hassle free. No longer do I have a single password, in fact, every password I have now is so complex, even I can’t remember it. The only password I need to remember now is the Lastpass one itself.(Review)”*

Some survey respondent referred to memory-related reasons for adopting password manager applications:

*“Because I always forget my passwords (Survey)”*

*“I use a lot of different passwords that I forgot after a while or when i have to change the password to another, i keep remembering the old one not the new one (Survey) ”*

*“My passwords are different for each account and difficult to remember them (Survey)”*

They said it helped to retrieve infrequently used passwords:

*“I’m no longer reluctant to create accounts for things I only rarely look at (because I don’t have to worry about remembering login credentials and passwords); I never have to try to remember what I used for security questions and answers (because I record all of that into OnePass) (Review)”*

or being used years ago:

*“If you’ve ever found yourself staring blankly at the “security questions needed to verify identity” password reset prompt, because you have absolutely no clue what your favourite food was 8 years ago, then do yourself a favour and download Lastpass (Review)”*

Moreover, password managers help their owners to construct strong passwords instead of trading off between memorability and security of their passwords:

*“It’s an incremental life-changer that actually lets you have stupid-complex passwords without having to remember them all (or use the same one over and over).(Review)”*

*“Now, instead of agonizing over a password I can remember vs. one that’s secure, I am able to choose secure every time (Review)”*

In addition, some reviewers reported that these tools eliminate the need for fallback authentication when they forget their passwords:

*“Even those ridiculous fallback questions (what’s your favourite movie... Like that’s never going to change!).*

*Even for my “mother’s maiden name”, I use secure random strings, unique per site, on most sites (Review)”*

#### **Typing difficulty (Effort Amelioration)**

One of the reviews referred to the difficulty related to entering a secure password when using a phone which emphasises the importance of using supportive tools, according to the reviewer:

*“shudder to think what it would be like to type an actually secure password on one of your phones (Review)”*

#### **Synchronisation (Perceived Usefulness)**

This feature was a strong reason for adopting these applications. This might be because of the fact that many users own multiple devices that they need to access their accounts from. For example:

*“and keep everything in sync on multiple devices and computers (Review)”*

While users, in general, referred positively to this feature in their reviews, some specifically gave evidence of their security awareness by being concerned about sending their passwords over the Internet. They prefer password managers that provide safe synchronisation. For example:

*“1password can work and sync with other 1password installations without ever sending a single password over the internet (Review)”*

However, some users indicated their preference for a variety of different synchronisation methods:

*“One thing that has bothered me for a long time that I don’t understand is the lack of options for syncing more than one vault. I don’t have a Dropbox account and even if I did, shouldn’t there be other ways to sync one of the vaults that may very well contain some sensitive information besides just Dropbox? I keep thinking one of these updates will address this issue but so far I am still unable to make use of a secondary vault because I don’t have a Dropbox account. Just doesn’t make sense.(Review)”*

#### **Privacy**

Those who posted positive ratings believe that their privacy is respected by the developers of the application:

*“you do not even have to tell them your email address (Review)”*

Some users believe that companies that provide these services have no interest in violating their users’ privacy:

*“which is equal parts awesome and scary, right? All your passwords passing through the ether, supposedly protected, out there for the NSA or some other mad scientist to steal. With convenience comes risk. That risk is yours to take (or not). The purveyors of this software have a vested interest in not screwing with the trust of its customer base. For that reason you can (arguably) trust them to be hyper-vigilant in the maintenance and security of this software (Review)”*

This shows that user perceptions of an application’s privacy preservation plays a role in their decision to adopt these kinds of tools.

#### **User interface (Perceived Ease of Use)**

The interface might contribute to influencing decisions to use a password manager:

*“The easy user interface, consistent quality and continual development keeps both desktop and phone/tablet software ahead of the competition (Review)”*

The participants who do not use password manager in their phone declared that the simplicity of the application might make it possible for them to start using these applications:

*“If I find a very simple app. With less text and more graphics (Survey)”*

However, some reviews referred to their bad impression of the user interface of some password manager applications. For example, this review is found in the 1password Android application:

*“why do I have to go very deep into the app before I can search for a login? That’s a very frequent user journey! (Review)”*

Interestingly, other reviewers said they liked the user interface of this particular application:

*“Most user friendly interface I’ve come across in terms of password managers(Review)”*

Moreover, the reviews reveal that users prefer less interaction from the application such as using their phone’s keyboard instead of using a bespoke keyboard:

*“I don’t want to use a different keyboard, but I do want to autofill (Review)”*

#### **Safe Sharing (Perceived Usefulness)**

Some reviews pointed out that password manager applications allowed them safely to share their passwords and important documents with their partners:

*“Because it’s securely synced to my Dropbox and shared with my wife, there’s never a worry about getting locked out of a site. We use it on all our devices (Review)”*

*“makes it a breeze to share logins with my wife, as well as store and use personal info (Review)”*

#### **Regular Updates to Meet User Needs (Perceived Usefulness)**

Many users like regular updates and continued improvements to fix flaws, improve usability, and introduce new features:

*“The other great thing is that the company continually improves and optimizes the app, making it constantly better, faster and even more useful (Review)”*

*“This application has never failed me yet and more importantly the app is regularly updated (Review)”*

This may encourage reliance on these applications.

#### **Customer support (Social Need)**

Many reviews indicated that the customer support delivered made a good impression. This can be clearly seen from the responses to user reviews. This might positively impact the user’s decision to continue using the system and meet the “relatedness” basic human need as can be seen in this review:

*“Their technical support truly listens to you. With most apps, you sometimes wonder if there is someone still on*

*the other end. If there is any problem they will fix it (Review)”*

*“they responded within minutes ! Their help was spot on correct, courteous, and quick (Review)”*

Moreover, some reviewers who were unhappy with the password manager referred to poor communication with the service provider:

*“contact support with a serious issue and they give you an unhelpful curt answer and when you try to follow up with a request for clarification they shut down the opportunity with a “status resolved” door slam in your face.(Review)”*

### **Transparency (Security)**

The reviews reveal that when a password manager reported an attack, the transparency in explaining how that was happening could increase user confidence in the application:

*“Security now also explained on a previous episode how LastPass was hacked; which calmed my nerves after listening to the episode (Review)”*

Transparency in explaining how the system manages their data can influence decisions to adopt these applications:

*“I didn’t trust these programs for a long time. Agile bits is very transparent about HOW your data is kept safe, so I started (Review)”*

One participant that open source code made the application more reliable:

*“Open source code and easy to understand description (survey)”*

### **Additional features (Perceived Usefulness)**

Many reviewers were impressed with the different options and functions available. They reported that these apps have not only changed their password usage behaviour but also provide extra security features that make their lives easier:

*“I have scanned and added many important documents such as birth certificates, auto insurance cards, social security cards, passports, drivers licenses, medication lists, banking info and much more. ALL of these items are available to me and my wife anywhere, any time with the touch of a screen, and they are all encrypted using 256 bit AES encryption (Review)”*

*“but it acts as a complete storage for everything important such as wallet items, router & server info, and much much more (Review)”*

### **Usability (Perceived Ease of Use)**

Due to security and/or usability requirements, the availability of the biometric fingerprint authentication mechanism seems to have had a big impact on usage of password managers. While iPhone users rated 1password because of the support of TouchID, Android users complained about the lack of support for biometric authentication, especially those who used 1password on their iPhone or had migrated from iOS. For example:

*“But there is no fingerprint support for Android. iOS version does have the fingerprint feature (Review)”*

Although some of the existing password manager applications already accept fingerprint authentication, some non-users said the incorporation of biometric authentication might make them start using these tools:

*“integration of the passwords with the fingerprint or any other biometric sensor (Survey)”*

*“If the password is my fingerprint or something like that.(Survey)”*

Some who used 1Password and password Saver applications claimed that they chose them because of the availability of the “fingerprint” feature:

*“No one can enter it unless with my finger print (Survey)”*

### **Feeling Secure (Security)**

The majority of the reviewers and survey respondents who do use password managers on their phones stated that these applications increased the security level of their online accounts:

*“it is really really really encrypted (Review)”*

Some said their search for ‘more safety’ or ‘security purposes’ in general made them use these applications. Others indicated the importance of the password generator function provided by these applications, in terms of maximising the security of their passwords, and thus helping them stay secure on the web by generating ‘long and complex’ passwords. For example:

*“use 1Password generated password and feel safe that you have a password that cannot be hacked and it still easy to use (Review)”*

*“1Password looks great, comes with a strong password generator to help my pick good passwords every time I change one (Survey)”*

Furthermore, some are aware of the importance of having ‘unique passwords’ for each account:

*“My passwords are different for each account (Survey)”*

Also, some stated that password manager applications prevent poor password behaviour:

*“stop using the cat’s name for every password on every site you access, and download this app (Review)”*

and make them aware of password weaknesses

*“Identify any password weakness or any password matching (Survey)”*

Some users pointed out the advantage of having a password manager when one of their accounts had been attacked, compared with the situation where they might have used the same password for more than one account. For example,

*“I use 1Password multiple times a day to recall and fill one of my 1600 or so unique and ridiculously complex passwords. If someone gives away one of my accounts, it is zero panic.(Review)”*

*“In summer 2014 when eBay passwords were compromised, I didn’t worry. My eBay password was unique to eBay so I new my other accounts were safe. I simply changed my eBay password and went on with my day. OnePass makes this all possible (Review)”*

Moreover, the fear of certain kinds of attacks, such as shoulder surfing attacks, may influence Smartphone users to adopt password manager applications:

*“Will prevent others to see my password while I type it (Survey)”*

#### **Social & Media Influence (Social Need)**

The media, such as podcast shows, can influence users to attempt using a password manager. For example:

*“What convinced me to try it was the Mac Power Users’ podcast #173 where they spent the whole hour on how useful 1Password is. Listen to that show and you will appreciate this app (Review)”*

Or it could persuade them to continue using the app

*“watched security now with the CEO of LastPass and after that interview I felt safe to still continue with LastPass (Review)”*

The reviews demonstrate the power of social influence in influencing user decisions about using password managers. The pronouncements of experts that users know from the media can play a role:

*“Steve Gibson will still be using LastPass and so will I (Review)”*

*“Just got done watching Joe on Security Now with Steve Gibson and Leo LaPorte. Joe is staying on with the team (Review)”*

Having those close to you interact with them directly also has an impact:

*“My husband encouraged me to download this app (Review)”*

*“I’ve recommended it in person to countless friends and they use and love it (Review)”*

*“Got multiple friends and family members to use their service (Review)”*

A number of participants who do not use password manager applications indicated that they might consider using them if they knew that other users were doing so:

*“If many people use it first without problems (Survey)”*

*“if it became popular and many people use it without any issues (Survey)”*

or if it was suggested by others:

*“suggested by closed friends (Survey)”*

*“friends recommendations (Survey)”*

Moreover one participant said “intervention of others” influenced her/him to use a password manager on her/his phone. This confirms the findings of [37] about the importance of our peers and significant others when it comes to Smartphone usage.

#### **Access (Perceived Usefulness)**

Users believe that using these applications ensure they are not locked out of a website, as they can access their accounts from any other device too. For example,

*“removes the aggravation that ensues from getting locked out of an account because of a lost password (Review)”*

Storing passwords in the cloud such as DropBox is seen as a positive feature since they can use their passwords from all their devices.

*“Now any computer or phone or tablet i use my passwords are stored and i can get to them (Review)”*

#### **Availability (Perceived Usefulness)**

password manager users reported in the reviews their satisfaction about having their password and important documents available at anytime:

*“I store passwords for sites, credit card details, passports and driving licence copies so I have them to hand 24/7 without the need to carry the originals, documents and secure notes.(Review) ”*

#### **C. Factors Leading to Rejection**

Here are the factors that deter smartphone users from starting to search about password manager application or reasoning them for not starting to think about adopting these tool:

##### **Poor or No Awareness**

Many participants did not know about the existence of these applications. Some examples of their responses are:

*“I have no idea about their existence; (Survey)”*

*“I did not hear about it before (Survey)”*

##### **I am already Secure (No Perceived Usefulness)**

Some participants said that they did not need to use password manager applications because they believed that their current password behaviours were secure:

*“I use one strong password for everything (Survey)”*

or they used other security tools such as one-time passwords:

*“I don’t feel I need it I use one-time password applications and I believe it is secure (Survey) ”*

In addition, some participants were confident in their ability to remember their passwords:

*“I don’t need it , can remember my passwords (Survey)”*

*“I can remember my passwords I use. And I would not feel safe with all passwords saved accessible through just one other password (Survey)”*

Some prefer to use the recovery function instead of a password manager:

*“Because I rarely forget my passwords, also I prefer if it happened and forgot the password to reset it (Survey) ”*

Moreover, some participants believe that they do not need these supportive security tools because they are already taking online protective action by visiting only what they believe to be trusted websites :

*“Because I do not think I need it. I visit only popular websites so I do not need very very complex password for them (Survey)”*

However, some participants mistakenly considered themselves to be secure. Here are some examples demonstrating that people thought using the same password for many accounts was secure behaviour:

*"I didn't need it yet. I always choose the same password. I am good at memorising numbers and codes (Survey)"*

*"I have one password for all my accounts ..i don't need to write it (Survey)"*

*"Because I use similar passwords for different accounts so I do remember my passwords (I don't feel I need it) (Survey)"*

*"I dont feel like I need it.I use strong passwords by myself and they are very similar, so i dont get confused (Survey)"*

#### **I have Few Passwords (No Perceived Usefulness)**

Some participants did not see the need to use password manager applications because they do not have many online accounts:

*"I use to memorize my password since I don't have too many (Survey)"*

*"Also, I have a few passwords to remember so I don't need an external help (Survey)"*

#### **Data is not Valuable (No Perceived Usefulness)**

Some participants consider their data not to be valuable:

*"No reason I do not have anything to worry about I do not want to bother myself with complicated passwords (Survey)"*

*"I have not got important things on my mobile (Survey)"*

*"Maybe if have important accounts like a bank account (Survey)"*

#### **Insignificance (No Perceived Usefulness)**

Some participants did not see the need to have strong passwords as they believed that their online accounts would not be attractive to attackers.

*"If I get rich or became a politician then I would think about strong passwords(Survey)"*

*"I believe that it is too much for me to have such applications, as i am not a celebrity or politician and therefore have no stalkers (Survey)"*

*"I don't use my Smartphone for my critical information. I prefer to use it as a communication device to call and message and browse on google, not to login into any important websites because i believe i might forget it somewhere. so i prefer to check emails and important login information through my desktop computer (Survey)"*

#### **Not wanting to be first**

As this tool is not widely known by smarphone users, many thought it was a recent development and they believed and thus did not want to be the first to take the risk in using such an applications:

*"Not that popular so it must be not that good (Survey)"*

*"If i see many people use it and like it or famous people use it and like it (Survey)"*

#### **Mastery**

Some participants attribute their decision not to use a password manager to their desire to challenge themselves by retrieving the right password from their memory.This can be explained

by Pink's motivation theory [38] as the human basic need for 'mastery'. It can also be illustrated by the need for 'competency', according to self determination theory [39].

*"I like to challenge myself by remember my passwords .. feel proud of myself it's not a joke! (Survey)"*

*"I do not like to depend on technology to remember all my passwords This will make my memory lazy (Survey)"*

#### **Security Concerns**

While many password manager application users believed that these applications maximised their online security, those who chose not to adopt these tools had concerns about their security:

*"I always feel that the security of these applications are not good (Survey)"*

*"I do not fully trust that the software will be able to provide enough security. After all, there is no such thing as an impenetrable security, especially in digital world. Should someone hack into my account, they will know all my passwords. Even though there is a risk that I will not be able to remember some of the passwords, then at worst, the data will just be lost (Survey)"*

Particularly, the fact that these type of systems have a single point of failure:

*"Risk of keeping all eggs in one basket (Survey)"*

*"May be because when the attacker can get inside the password manager, he/she can take all my passwords.But when attacker get one password and get inside my email that will be more secure because I only lose the access to my email account only not all accounts (Survey)"*

*" It is a risky application if master key is attacked then every thing gets lost (Survey)"*

*"... its going to be easier for other people to hack my account since they can get the password from the password manager (Survey)"*

They worry that these types of systems might attract attackers:

*"I don't like the idea of having all my passwords stored in one place (The password manager app) which will be most likely on the list of hackers to crack and if they already did crack it, it will obviously be the first thing they will look for after attacking my PC or Phone and that doesn't quite feel safe, nor assuring. To me using a word document that doesn't look like anything special feels safer and you can lock it with a password too (Survey)"*

*"I don't trust applications. Hackers may use these kinds of applications to achieve their personal and illegal goals (Survey)."*

or even if it lands up in the hands of another person:

*"My accounts are very important to me and cannot trust putting them in danger of getting lost if my phone get damaged or stolen (Survey)"*

*"Because my cell phone is sometimes used by my children and other family members there is a risk to use it (Survey)"*

Also some participants believed that their phone itself was not secure; that it might have viruses that could affect their passwords if they used a password manager:

*“It’s a security matter. I use it in my computer because it has anti virus and firewall and sometimes when I google a website it tells me which website is risky. My phone has non of these things and I have some applications in my phone games that I believe they are not very safe (Survey)”*

*“Cuz my phone got viruses and not safe (Survey)”*

Also, they seem aware of the security risk of using public Internet services :

*“I use public wifi networks which make it much easier for attackers to attack my passwords if I used password manager application(Survey)”*

In addition, users seem unsure about their current security knowledge and information and thus do not want to put themselves at risk of having yet another critical application to look after:

*“advices how to stay secure when using it (Survey)”*

### **Privacy Concerns**

While some reviewers show their confidence about preserving their privacy by the service providers as explained earlier, some of those who chose not to adopt password manager cited privacy concerns a lack of trust in the vendors. For example,

*“personally I don’t know anything about the developers or the app source (Survey)”*

*“I don’t trust these application.They made in U.S. to know everything about us.Now they know everything but not passwords so they made this application to trick us. If you see imges of Google data centre you will not use these kinds of systems anymore (Survey)”*

*“Because I don’t trust the software not to collect my passwords for itself (Survey)”*

*“I dont trust it, as I am not sure about the developers of this app and what they can do with my details (Survey)”*

Also, some stated that if they trusted the developers then that would make it possible for them to use these applications:

*“May be if it is:..from a trustful source (Survey)”*

For example if it is developed by a well known organization:

*“A password manager that is developed by popular companies like google, apple (Survey)”*

*“If distributed by trusted source or big industry name like apple keychain (Survey)”*

or developed by people who they trust

*“Nothing will make me use it unless I develop it myself or someone trusted like people in universities (Survey)”*

others said if the application was open source they might use it:

*“Open source code and easy to understand description (Survey) ”*

However, one of the reviews referred to the importance of trading off between privacy concerns and their security password behaviour:

*“This is not an app for nerds, geeks or those who overdramatise the importance of internet security. Put simply, if you care in any way for your personal privacy and / or the stuff you store and access online, you need to wise up, stop using the cat’s name for every password on every site you access, and download this app (Review)”*

Smartphone users may encounter some factors that affect their decision to adopt one of the available password manager applications:

### **Uncertainty**

Some participants who not use these applications referred to a lack of understanding about how these applications build and work, which constitute a barrier in terms of trusting these tools:

*“...After I did a quick reading about it I have an idea but I do not know how it works? I don’t mean how I use it but how this application takes my passwords and make them strong and where are they kept? Is it in America? All these things I need to know before trusting these applications (Survey)”*

*“.. not understand how they are implemented; the available information for these application is complicated and not clear (Survey)”*

*“More elaboration on how to really function with less complicated terms of agreement (Survey)”*

In some cases, smartphone users might be thought of using password manager applications and adopted one of these tools but then uninstalled it. These are some factor that influenced their decision:

### **Device Speed (Negative Features)**

According to the reviews, some Smartphone users complained about the efficiency of their devices after installing and using password manager applications:

*“Also for some reason it makes my Mi 3 significantly slow when it is running on the background, so only three stars for now.(Review)”*

*“According to System Panel this app is using a lot of CPU cycles even though it’s not being used that much (the icon does keep coming up in the status bar for no known reason). Considering uninstalling, at least temporarily as an experiment (Review)”*

### **Device Memory & Battery (Negative Features)**

As the memory size on Smartphones is relatively small compared with other computer devices users are careful about apps they install. They only use applications that they believe they need. Some users indicated that they did not have enough space to install a password manager application. For example:

*“Takes up a lot of battery and RAM (Survey)”*

*“i am enough with using application,i use note or my mind (Survey)”*



*“I don’t have enough space in my phone Even i delete the applications that I have in my phone when I need memory to capture a moment for my kids and then I re-install the apps later when I find space. In the case of password manager I can’t do that! (Survey)”*

In the review, one of the users pointed out the preference of having lastPass over Dashlane application because of their size:

*“Lighter than Dashlane, which makes LastPass more preferable than Dashlane (Review)”*

Some participants expressed concern about apps consuming the battery:

*“latest version sucks more battery than the screen! Have it force stopped on phone, just turn it on when I need it (Review)”*

Battery consumption clearly negatively affects the users experience.

### **Connectivity (Negative Features)**

Some users indicated that having a poor Internet connection was a usage barrier:

*“Poor Internet in my country I do not want to use online password account each time I want to access one of my accounts. This will double my online access +sometimes I want to access my email to know something but I don’t have Internet in my place so I call one of my family member to see my email If my password is in this application then how can they access my email (Survey)”*

An Android user who had already adopted LastPass complained about the Internet connection. This clearly impacts their experience and the continued adoption of these tools:

*“Very nice and convenient app that let you save all of your passwords. But very difficult to access it when the Internet connexion is poor.(Review)”*

### **Differences Across Platforms (Negative Features)**

Many reviews claimed that developers only focused on iOS but not Android and they considered the Android version to be inferior to the iOS one. Some reviewers complained about the lack of features such as fingerprint authentication in the Android version of 1Password, especially those who used the same application on the iOS platform:

*“I have this on all my iOS/OSX devices and it’s so much nicer on those platforms.... Only reason I’m even using it on Android is all my stuff is already saved to it from Apple devices. I wouldn’t have given this app a shot at all if it wasn’t for the other version hooking me in (Review)”*

Another review on LastPass:

*“But there is no fingerprint support for Android. iOS version does have fingerprint feature (Review)”*

Another negative review is about paying for the same application on each different platform while the point is to synchronise passwords across devices:

*“Bit tired of having to pay for each different OS. Isn’t the whole point of this app to be able to sync credentials*

*across devices and operating systems? Bit cheeky then to charge extra for that (Review)”*

### **Linkage with Other 3rd Party Services (Negative Features)**

In the reviews, some users complained about having to use an additional account with a specific service provider such as DropBox in order to be able to synchronize their passwords across other platform and some suggested other preferable methods like Wi-Fi sync or accounts e.g. iCloud and Google Drive:

*“My understanding is that I must use Dropbox to sync the vault on mobile. Since I don’t use my Dropbox on my work computers, this makes complete sync impossible (Review)”*

*“Then, they took away WiFi sync and added iCloud – except the desktop doesn’t support iCloud yet. So there’s no real migration path. I don’t want to have to install 3rd party dropbox accounts and junk to make this work. WiFi should be included until they get iCloud in the desktop then they can do away with WiFi. But this is terrible and leaves me with mobile devices now that can’t sync with my desktop anymore! (Review)”*

### **Country-Specific Features (Negative Features)**

Reviewers pointed out that some features in the password manager are exclusive to a certain community and therefore it affects their experience:

*“I would like to see change would be a better selection of items for a global community rather than this extremely American feel to data capture. So UK NI number, drivers licence etc. Not just UK but other countries (Review)”*

*“App can’t cope easily with uk type of banking password structures which cycle at each login, crashes internet explorer frequently requiring a laptop reboot and freezes regularly (Review)”*

### **They are not supported by other web accounts (Negative Features)**

Lack of support from other service providers may affect Smartphone user willingness to rely on these tools for managing their passwords. Some reviews claim that they found applications and web sites that are not supported by the applications such as

*“The only problem is with iOS and more crucially with web and app developers who don’t support this. Everyone needs to complain when they come upon web sites that prevent password managers from seamlessly entering passwords and credit card info (Review)”*

Some websites, such as British Gas, do not support the use of any password managers on their login page. This might be a barrier for some to integrate in using these applications.

### **Uncertainty**

Some people don’t know enough to deploy these applications. This might be due to usability issues. For example, some users lacked confidence:

*“If you asked me how to get a credential from 1P into any other app, I wouldn’t be able to tell you (Review)”*



*“Because I can not understand how I can use it for my account that I use now. I use the google one in my computer because it already pop up and ask me do you want to save your passwords . Even though it can’t help me to make a strong ones (Survey)”*

### **Cost**

In some cases in the reviews and the survey, the cost was a barrier to adopt these systems. They stated that they are unready to pay so much for a secure password manger when other password mangers are free. For example this review is found in 1Password in UK Apple Store:

*“I planned to buy it for my partner but the price seems a fair bit higher (Review)”*

*“Being free of charge.(Survey)”*

On the other hand, in some other reviews, users hesitated to trust their passwords to free applications, they believes that free apps were not really free, and some have tracking included. They also feel that most free applications have security weaknesses:

*“Are you sure you trust your password to a free app? Free apps aren’t really free, some have tracking included, pesky advertisements, or they might report back to the “mother ship” (Review) ”*

### **Time Commitment (Perceived Effort)**

For many users, security is a secondary task required primarily in order to complete their primary task [40]. Therefore, people are less willing to spend time reading about how this tool works or how to use it. Moreover, people do not have time to think about the accounts they have and each associated password. Quotes from the participants’ responses suggest that time might be a barrier to adoption:

*“I don’t have time to search more about it ;so it better leave it (Survey)”*

*“I don’t have time to find my accounts and each password and give them to the password manager (Survey)”*

### **Control**

Some users were concerned about not being able to maintain control over their passwords when using a password manager. This can be explained, according to self determination theory [39] and Pink’s Motivation theory [38], by the human need for ‘autonomy’ when interacting with the digital world. Autonomy is defined as the sense of freedom and control over ones own choices. This can be seen in these responses to the question about the reason for not using these applications:

*“I prefer to keep my password under my control.(Survey) ”*

*“Password manager is not good you can lose control of your passwords.(Survey) ”*

*“Fear of not being able to have control over my passwords in case it’s being attacked or I forget the master key.Fear of being under the control of this app developer. (Survey)”*

Moreover, due to the fact that some of these applications do not provide a recovery plan for the master key, some users

post negative reviews about not being able to control their passwords:

*“Recovery options terrible..Just set it up. Worked fine until I logged out and could not quite get password right. Now totally inoperable. Cannot login cannot reset cannot delete account and start over. Electronic version of a paperweight. (Review)”*

*“What if I forget the master password? (Review)”*

### **D. Reprise of Adoption Factors**

Section II-3 identified a number of adoption factors from the literature, as summarised in Table I. Our findings confirmed a number of contextual, psychological and sociological factors but did not detect anything that hinted at an interest in new technologies impacting adoption. We did not explicitly test for hedonic or age-related factors. This does not mean that they are not influential, only that they did not emerge from our analysis. In fact, we believe that they could provide a fruitful avenue for further attention since they have proved influential in other contexts, and might well encourage adoption in this context too.

## **V. DISCUSSION**

We identified a number of factors influencing password manager app adoption in different phases of the application lifecycle. A number of these confirm the findings of [41]. Certainly lack of awareness was a strong theme in both studies. People will not even embark on the life cycle depicted in Figure 1 if they do not know of the existence of password manager tools. The lack of awareness is puzzling since these applications have been available since 1999 [42]. Due to the sensitivity of password data and with so few people using them, it is unlikely that they are hearing about the apps from friends and family. So, how would people become aware of these apps?

Some of the reviews said adopters recommended the password manager to others, so if a certain critical mass of people start using them, many more will probably follow. Also, some of reviewers spoke about hearing about famous people using password managers and said that they adopted them as a consequence. There is a clear need for effective marketing if more people are to adopt these tools.

However, even if people become aware of the apps, they might still not embark on a search process to consider installing one. Many people mistakenly think their current password practice is secure [43]. Some participants believed that they did not need security support tools because they only used one password for all their accounts. It seems that, in addition to making people aware of these password manager apps, we should also work on disseminating “good practice” with respect to password behaviour so that they understand their current behaviour is making them vulnerable to attack.

This study revealed factors that might deter adoption even if users have heard about the app, and were sufficiently interested in using the tool. A number of our respondents did not understand how this application worked and was used. Due

TABLE I  
ADOPTION AND REJECTION FACTORS IDENTIFIED IN THIS STUDY

	ADOPTION Factors	REJECTION Factors
Contextual	Time, Ease of Use, Perceived Usefulness, Perceived Effort Amelioration, Experience	No perceived usefulness, Negative Features, Cost, Perceived Effort
Psychological & Sociological	Subjective Norms, Social Need, Security, Privacy	Not wanting to be first, Privacy Concerns, Security Concerns, Competency, Control, Mastery, Uncertainty

to the critical nature of the data manipulated by password managers, users need to be able to trust these systems and they need to know how their passwords are secured and stored, at the very least. It is unfortunate that most of the existing applications in App stores fail to report how these password manager actually work. Anaylew reports that Apple consumers consider the description and the screenshots in App Store Product Pages when they are interested in buying an application [44]. One reviewer suggested the use of video clips to improve the user experience. Yet most of existing password manager applications in Apple and Google play stores only provide a description of how the application is used. A few provide screenshots of the application interface and they mostly focus on demonstrating the features provided by these tools. They seldom explain how the data is secured. Only a few provide demonstration videos: 1password and mSecure in the Apple store and DashLane and RoboForm in Google Play store.

Other users felt that such a password manager would violate their basic human needs of autonomy, mastery and competency. Humans need to retain control [45, 38] and password management is no different. It might be that in trying to be helpful by taking away all password-related concerns these apps make people feel that they have lost the sense of control they need. Password managers might need to work on giving people a sense of control during operation.

We should also briefly consider the hedonic quality of these apps, mentioned by [21] as an adoption factor. No one in our surveys and reviews spoke about the app being “enjoyable”, yet this is clearly something people want. They spoke about being reassured, the reduction of effort, the relief of not having to manage passwords, but no mention was made of enjoyment. Hassenzahl *et al.* polled 548 people and reported that hedonic quality was strongly associated to positive experience of an app [46]. This is yet another non-functional quality that app developers could pay attention to, in order to improve adoption.

Future research should consider the following research directions:

**SEARCH:** How can password managers be advertised more effectively to build up a critical mass of users who could, in turn tell other users about this kind of application?

**DECIDE:** How should password manager apps be described in the app stores so as to engender trust in users engaged in the decide phase of the life cycle?

**TRY:** Two questions arise. (1) How can password managers be designed so as to give the user a sense of retaining control over his/her passwords? (2) How can password managers be designed with enjoyment in mind?

## VI. LIMITATIONS AND FUTURE WORK

There are some limitations to this study that have to be acknowledged. In the first place, we deployed snowball sampling to recruit respondents, so our sample can not be considered representative of the entire population. Hence the factors this exploratory study revealed will have to be confirmed with a wider-ranging study, consulting a more representative sample.

The online survey did not consider cross-cultural differences. This is relevant because people might well be influenced in their adoption decisions by country- or culturally-specific factors. For example, in some Nordic countries the eID is used as a country-wide two-factor authentication method. A cross-cultural study is needed to ensure the validity of adoption and rejection factors in other cultures.

We did not collect demographics in the online survey. We did this to encourage full disclosure, but this also meant we could not explore gender or age differences in responses. Future studies will need to pay attention to these factors.

The study did not attempt to weight the impact of the different factors on adoption and rejection, nor did we attempt to map factors to actual usage. These aspects will have to be explored in follow-up studies.

## VII. CONCLUSION

Password managers can ameliorate password management difficulties experienced by Smartphone users. Cost is no bar to their use, since many are free. Yet, despite the obvious benefits, widespread adoption has not occurred. We examined online reviews of password managers and elicited opinions from 352 respondents. A number of factors impacting adoption were identified. Poor advertisement and a failure to reassure potential users about the trustworthiness of these applications could well explain the poor uptake of these tools. Moreover, the analysis reveals that designers should pay more attention to the user experience. The factors reported in this paper can help developers to design and market systems to encourage adoption.

## ACKNOWLEDGEMENT

We want to thank Rosanne English for her very helpful comments on an earlier draft of this paper.

TABLE II  
A REVIEW OF SMARTPHONE PASSWORD MANAGER APPLICATIONS

	LastPass	1Password	iCloud Keychain	DashLane	mSecure
Synchronisation	Premium	Dropbox, iCloud, Local Folder ,Wifi	only Apple devices	Optional	Optional
Cloud	Yes	Optional	Yes	Optional	Optional
Auto Populate	Optional	Optional	Optional	Optional	Optional
Credentials	Email Address for Cloud Account	None	Email & Phone Number	Email	Email for Backup
Storage	Own Cloud Service	Local Device	Cloud	Local or Dashlane Servers	Local or Cloud
Encryption	AES 256-bit	AES 256-bit	AES 128-bit	AES 256-bit	Blowfish 256-bit
Generator	Optional	Optional	Optional	Optional	Optional
Authentication	Premium	Fingerprint, one-time (Pro)	No	Fingerprint	N/A
Recovery	Email Hint	Hint display after 4 wrong passwords	No Recovery	Reset Account	Password Hint
Password Strength	8 Character	None	4 Character	8 Character with 3 types	None
Cost	Free or 8.99/year for premium	Free or Pro (7.99)	Free	Free or Premium (29.99 a year)	iOS:7.99 Android:6.99
Rating	Google play: 4.6 (62350 rating) US: 3.5 (2476) UK: 3.4 (294 ratings)	App store: UK: 4.5 * ( 2322 Ratings) US: 4.5 (14912 Ratings) Google play: 4.3 (17033 rating)	N/A	UK: 4.4 (985 rating) US: 4.4 (10605 Ratings) Google play: 4.5 (30599 rate)	US: 5 (27 Ratings) UK: 4.4 (1339 ratings) Google play: 4.5 (9275)

## REFERENCES

- [1] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999.
- [2] P. Hoonakker, N. Bornoe, and P. Carayon, "Password authentication from a human factors perspective: Results of a survey among end-users," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 53, no. 6, pp. 459–463, 2009.
- [3] E. von Zezschwitz, A. De Luca, and H. Hussmann, "Honey, I shrunk the keys: influences of mobile devices on password composition and authentication performance," in *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational*, pp. 461–470, ACM, 2014.
- [4] H. S. Al-Sinani and C. J. Mitchell, "Using CardSpace as a password manager," in *Policies and Research in Identity Management*, pp. 18–30, Springer, 2010.
- [5] P. Gasti and K. B. Rasmussen, "On the security of password manager database formats," in *Computer Security–ESORICS 2012*, pp. 770–787, Springer, 2012.
- [6] A. Das and H. U. Khan, "Security behaviors of smartphone users," *Information & Computer Security*, vol. 24, no. 1, pp. 116–134, 2016.
- [7] N. O. Alshammari, A. Mylonas, M. Sedky, J. Champion, and C. Bauer, "Exploring the adoption of physical security controls in smartphones," in *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pp. 287–298, Springer, 2015.
- [8] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? security awareness in smartphone platforms," *Computers & Security*, vol. 34, pp. 47–66, 2013.
- [9] S. Furnell, "Why users cannot use security," *Computers & Security*, vol. 24, no. 4, pp. 274–279, 2005.
- [10] N. Alkaldi and K. Renaud, "Why do People Adopt, or Reject, Smartphone Security Tools?," in *Proceedings of the 10th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016)*. Frankfurt, Germany, July 19-21 2016.
- [11] A. A. Al-Daraiseh, D. Al Omari, H. Al Hamid, N. Hamad, and R. Althemali, "Effectiveness of iPhones Touch ID: KSA case study," *Editorial Preface*, vol. 6, no. 1, 2015.
- [12] S. Chiasson, P. C. van Oorschot, and R. Biddle, "A usability study and critique of two password managers.," in *Usenix Security*, vol. 6, 2006.
- [13] W. Prata, A. de Moraes, and M. Quaresma, "Users demography and expectation regarding search, purchase and evaluation in mobile application store," *Work*,

- vol. 41, no. Supplement 1, pp. 1124–1131, 2012.
- [14] G. Häubl and V. Trifts, “Consumer decision making in online shopping environments: The effects of interactive decision aids,” *Marketing science*, vol. 19, no. 1, pp. 4–21, 2000.
- [15] M. Böhmer, B. Hecht, J. Schöning, A. Krüger, and G. Bauer, “Falling asleep with Angry Birds, Facebook and Kindle: a large scale study on mobile application usage,” in *Proceedings of the 13th international conference on Human computer interaction with mobile devices and services*, pp. 47–56, ACM, 2011.
- [16] S. Nikou, “Mobile technology and forgotten consumers: the young-elderly,” *International Journal of Consumer Studies*, vol. 39, no. 4, pp. 294–304, 2015.
- [17] M. Hassan, R. Kouser, S. S. Abbas, and M. Azeem, “Consumer Attitudes and Intentions to Adopt Smartphone Apps: Case of Business Students,” *Pakistan Journal of Commerce and Social Sciences*, vol. 8, no. 3, pp. 763–779, 2014.
- [18] H. . Yang, “Bon appétit for apps: young american consumers’ acceptance of mobile applications,” *Journal of Computer Information Systems*, vol. 53, no. 3, pp. 85–96, 2013.
- [19] A. Y.-L. Chong, “A two-staged SEM-neural network approach for understanding and predicting the determinants of m-commerce adoption,” *Expert Systems with Applications*, vol. 40, no. 4, pp. 1240–1247, 2013.
- [20] T. Tsu Wei, G. Marthandan, A. Yee-Loong Chong, K.-B. Ooi, and S. Arumugam, “What drives Malaysian m-commerce adoption? An empirical analysis,” *Industrial Management & Data Systems*, vol. 109, no. 3, pp. 370–388, 2009.
- [21] A. K. L. Kit, *UTAUT2 influencing the behavioural intention to adopt mobile applications*. PhD thesis, Universti Tunku Abdul Rahman, 2014.
- [22] L. Dennison, L. Morrison, G. Conway, and L. Yardley, “Opportunities and challenges for smartphone applications in supporting health behavior change: qualitative study,” *Journal of medical Internet research*, vol. 15, no. 4, p. e86, 2013.
- [23] J. M. Vaterlaus, K. Barnett, C. Roche, and J. A. Young, ““Snapchat is more personal”: An exploratory study on Snapchat behaviors and young adult interpersonal relationships,” *Computers in Human Behavior*, vol. 62, pp. 594–601, 2016.
- [24] L. Piwek and A. Joinson, ““What do they Snapchat about?” Patterns of use in time-limited instant messaging service,” *Computers in Human Behavior*, vol. 54, pp. 358–367, 2016.
- [25] B. Xu, P. Chang, C. L. Welker, N. N. Bazarova, and D. Cosley, “Automatic Archiving versus Default Deletion: What Snapchat Tells Us About Ephemerality in Design,” in *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, pp. 1662–1675, ACM, 2016.
- [26] D. G. Taylor, T. A. Voelker, and I. Pentina, “Mobile application adoption by young adults: A social network perspective,” *International Journal Of Mobile Marketing*, no. 2, pp. 60–70, 2011.
- [27] J. Cho, M. M. Quinlan, D. Park, and G.-Y. Noh, “Determinants of adoption of smartphone health apps among college students,” *American journal of health behavior*, vol. 38, no. 6, pp. 860–870, 2014.
- [28] S. Thavalengal and P. Corcoran, “User authentication on smartphones: Focusing on iris biometrics.,” *IEEE Consumer Electronics Magazine*, vol. 5, no. 2, pp. 87–93, 2016.
- [29] M. Sandholzer, T. Deutsch, T. Frese, and A. Winter, “Predictors of students self-reported adoption of a smartphone application for medical education in general practice,” *BMC medical education*, vol. 15, no. 1, p. 1, 2015.
- [30] M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, “Its a hard lock life: A field study of smartphone (un)locking behavior and risk perception,” in *Symposium On Usable Privacy and Security (SOUPS 2014)*, pp. 213–230, 2014.
- [31] Google, “Google Play Store.” Accessed: 25th Nov 2015.
- [32] Apple, “iTunes Apple Store.” Accessed: 25th Nov 2015.
- [33] E. Ha and D. Wagner, “Do Android users write about electric sheep? examining consumer reviews in Google Play,” in *Consumer Communications and Networking Conference (CCNC), 2013 IEEE*, pp. 149–157, IEEE, 2013.
- [34] D. Yoganathan and S. Kajanan, “Designing Fitness Apps Using Persuasive Technology A Text Mining Approach,” in *Proceedings of the 18th Pacific Asia Conference on Information Systems*, 2015.
- [35] G. Hofstede and M. H. Bond, “Hofstede’s culture dimensions an independent validation using Rokeach’s value survey,” *Journal of cross-cultural psychology*, vol. 15, no. 4, pp. 417–433, 1984.
- [36] A. Bowling, “Mode of questionnaire administration can have serious effects on data quality,” *Journal of public health*, vol. 27, no. 3, pp. 281–291, 2005.
- [37] K. Renaud, R. Blignaut, and I. Venter, “Smartphone owners need security advice. how can we ensure they get it?,” in *CONF-IRM - Cape Town, South Africa*, 18–20 May 2016.
- [38] D. Pink, “Drive: The Surprising Truth About What Motivates Us,” *New York: Penguin Group, Inc*, vol. 138, p. 240, 2009.
- [39] R. M. Ryan and E. L. Deci, “Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being.,” *American Psychologist*, vol. 55, no. 1, p. 68, 2000.
- [40] A. Whitten and J. D. Tygar, “Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0.,” in *Usenix Security*, vol. 1999, 1999.
- [41] M. Volkamer, K. Renaud, O. Kulyk, and S. Emeröz, “A socio-technical investigation into smartphone security,” in *International Workshop on Security and Trust Management*, pp. 265–273, Springer, 2015.

- [42] Roboform.com, “Password manager.” Accessed: 15 th April 2016.
- [43] B. Ur, S. Bees, L. Bauer, N. Christin, and L. F. Cranor, “Do users’ perceptions of password security match reality?,” in *CHI*, 2016. To Appear.
- [44] R. Ayalew, “The Paradox of Overfitting,” Master’s thesis, Human Computer Interaction Programme, Uppsala University, 2011.
- [45] M. Hassenzahl, “User experience (UX): towards an experiential perspective on product quality,” in *Proceedings of the 20th International Conference of the Association Francophone d’Interaction Homme-Machine*, pp. 11–15, ACM, 2008.
- [46] M. Hassenzahl, S. Diefenbach, and A. Göritz, “Needs, affect, and interactive products - facets of user experience,” *Interacting with Computers*, vol. 22, no. 5, pp. 353–362, 2010.

# When SIGNAL hits the Fan: On the Usability and Security of State-of-the-Art Secure Mobile Messaging

Svenja Schröder  
University of Vienna  
Email: svenja.schroeder@univie.ac.at

Markus Huber, David Wind, Christoph Rottermann  
St. Pölten University of Applied Sciences  
Email: {markus.huber, is121030, is121023}@fhstp.ac.at

**Abstract**—In this paper we analyze the security and usability of the state-of-the-art secure mobile messenger SIGNAL. In the first part of this paper we discuss the threat model current secure mobile messengers face. In the following, we conduct a user study to examine the usability of SIGNAL’s security features. Specifically, our study assesses if users are able to detect and deter man-in-the-middle attacks on the SIGNAL protocol. Our results show that the majority of users failed to correctly compare keys with their conversation partner for verification purposes due to usability problems and incomplete mental models. Hence users are very likely to fall for attacks on the essential infrastructure of today’s secure messaging apps: the central services to exchange cryptographic keys. We expect that our findings foster research into the unique usability and security challenges of state-of-the-art secure mobile messengers and thus ultimately result in strong protection measures for the average user.

## I. INTRODUCTION

Tools to securely communicate over the Internet, using end-to-end (e2e) encryption, have been available for decades. End-to-end encryption ensures that sensitive encryption keys never leave users’ devices, and communication providers are therefore unable to read exchanged messages. The first generation of end-to-end encryption tools, such as PGP, however lacks widespread adoption due to their bad usability [1], [2], [3], [4]. Since the first release of PGP three decades ago, two important aspects of secure messaging changed: everyday communication via mobile devices continued to grow as smartphones replace PCs [5] and the general awareness for privacy and security increased.

The trend of communication via mobile devices and the growing awareness for online privacy led to a number of new secure mobile messengers. The Electronic Frontier Foundation (EFF) provides an overview on the security properties of current mobile messengers [6]. From a security perspective, state-of-the-art mobile messengers can be split into two categories: messengers that provide client to server encryption

and messengers with end-to-end encryption. The first category of messengers allows service providers to read exchanged messages, while the second group ensures that messages can not be read by service providers. State-of-the-art end-to-end encrypted mobile messengers only require users to authenticate via their mobile number; the generation and exchange of cryptographic keys is handled transparently by the applications. The transparent end-to-end encryption of messages makes strong encryption accessible to the masses but also creates new security challenges. As compared to PGP, state-of-the-art secure mobile messenger applications rely on centralized services to provide the cryptographic identities of its users. This modus operandi results in the following security challenge: if the key-exchange service is tampered with, either willingly or by an attacker, the overall security of systems is subverted. In order to account for the compromise of the key-exchange service, mobile messaging apps therefore offer the possibility to verify the cryptographic identities of other users ultimately to establish the trust of exchanged encryption keys.

To the best of our knowledge we are the first to study the unique usability challenges of mobile end-to-end encrypted messengers. Specifically, we perform a user study on SIGNAL for Android [7]. SIGNAL originated from two separate mobile applications [8] — TextSecure (encrypted instant messaging) and RedPhone (encrypted phone calls). Due to its strong encryption protocols and the availability of its source code under an open source license, SIGNAL has become an important tool for users who face surveillance [9]. In April 2016, the currently most popular messenger app WHATSAPP [10], rolled out end-to-end encrypted messaging, based on SIGNAL’s protocol, to more than one billion users [11]. SIGNAL’s encryption protocol thus became the de facto standard for end-to-end encrypted mobile messaging. In this paper we present a usability study of the messaging app SIGNAL including an exploration of the users’ abilities to notice, handle and mitigate man-in-the-middle (MITM) attacks during usage. Our MITM attack simulates a compromised key-exchange service to ultimately evaluate the usability of SIGNAL regarding the detection and mitigation of such attacks. Our paper makes the following main contributions:

- We performed a user study with 28 participants on the usability of SIGNAL’s security features, the state-of-the-art application for secure mobile messaging.
- Our results showed that 21 of 28 participants failed to

compare encryption keys to verify the identity of other users. The majority of these users however believed they succeeded while in reality they failed.

- Finally, we suggest improvements for the usability of SIGNAL to better counter attacks on SIGNAL.

## II. BACKGROUND

SIGNAL offers forward secrecy at the same time as asynchronous message exchange. As such SIGNAL combines the PGP-like asynchronous messaging with the security properties of the OTR protocol [12]. Figure 1 shows a simplified description of the SIGNAL protocol, which is divided into three phases (registration, session setup, and message exchange). We point the interested reader to Frosch et al. [13] for a detailed analysis of SIGNAL’s protocol.

Alice and Bob want to use SIGNAL to exchange end-to-end encrypted messages. ❶ Alice installs SIGNAL and verifies her mobile number at the SIGNAL Server with either a verification text message (SMS) or a voice call. Once verified, Alice creates different sets of keys: a longtime asymmetric key-pair called Identity Key Pair, 100 ephemeral key pairs called One-Time Pre Keys as well as one Signed Pre Key which is signed with the Identity Key. SIGNAL automatically uploads Alice’s Signed Pre Key as well as the 100 One-Time Pre Keys to its server. ❷ Alice attempts to establish a session with Bob and therefore requests a Pre Key Bundle for Bob and Bob’s Identity Key from SIGNAL’s central service. The Pre Key Bundle consists of a single public One-Time Pre Key and the Signed Pre Key of Bob. Based on the One-Time Pre Key and the Signed Pre Key, Alice derives a symmetric Master Key for future communication, and stores Bob’s Identity Key. ❸ Based on the Pre Key Bundles of each other, both Alice and Bob derive the same Master Key, which is used to create ephemeral Message Keys for the actual message exchange.

The unique long-term Identity Key pair remains the same as long as the user does not delete it by for example re-installing the SIGNAL application. These Identity Keys are essential to verify the identity of communication partners. The SIGNAL application therefore stores the Identity Keys of other users as soon as a secure session has been successfully established. SIGNAL allows users to view this Identity Key within the application. In order to make sure that communicating parties received the correct Identity Keys, both parties have to verify the public Identity Keys via an out-of-bound channel (e.g. meet in person or via phone). This can be done by comparing the hexadecimal representation of the key byte per byte or by scanning the QR code of each other’s Identity Keys in person.

### A. Threat Model

Our threat model accounts for the compromise of SIGNAL’s central services. This compromise can be the result of targeted attacks on SIGNAL’s service infrastructure or assistance of SIGNAL’s team to a subpoena request. The compromise of SIGNAL’s key server results in two different possible attacks:

- ❶ **Attacks on the first session setup** do not result in direct user feedback. This attack can only be detected by **manually**

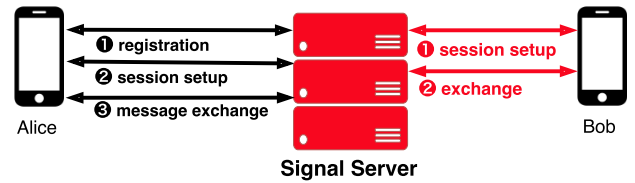


Fig. 1. Exchange of encrypted message with SIGNAL: a central service is used to exchange the public encryption keys — this service is critical for SIGNAL’s security.

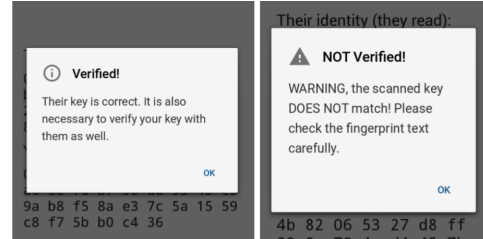


Fig. 2. Verification of Identity Keys by scanning the each other’s QR codes. On the left: a successful verification. On the right: Warning because Identity Keys did not match.

**verifying** e.g. over the phone or face-to-face via scanning the QR codes. Consider Bob wants to initialize a secure session with Alice, and Bob receives the attacker’s Identity Key (Mallory’s Identity Key) instead of Alice’s Identity Key which is then stored by SIGNAL as Alice’s identity.

- ❷ **Attacks on established sessions** where Bob has previously established a secure session with Alice and stored Alice’s correct Identity Key. An attacker (Mallory) could force both parties to re-negotiate a new communication session. In this scenario the compromised SIGNAL server would respond with the attacker’s Pre Key Bundle including the Signed Pre Key of the attacker, and thus establishes a man-in-the-middle attack.

SIGNAL accounts for both of the attack scenarios of our threat model. First, SIGNAL provides a feature to manually verify established Identity Keys, outlined in Figure 2. Second, SIGNAL warns users when it detects that long-term keys of users change, see Figure 3. In our paper we study exactly how usable and effective these two countermeasures of SIGNAL are.

## III. EXPERIMENTAL DESIGN

We conducted a user study in a laboratory setting in order to explore the usability of SIGNAL regarding its security features. Our study consisted of two parts: a usability study of the SIGNAL app with focus on SIGNAL’s instant messaging and security features, and the execution of an actual MITM attack with a subsequent assessment of the users’ reactions. To gain insights into the participants’ motivations, strategies and goals they were asked to constantly comment aloud on their actions with the Think Aloud method [14], which facilitated to understand the users’ mental models. User interaction and voice were recorded with a camcorder. Participants had to fill out a consent form before the start of the study, as well as a short questionnaire including demographics and general attitude towards privacy and security regarding smartphones and especially messaging apps. The study took place in the usability lab of the COSY Research Group at the University

of Vienna, which provides two lab rooms for usability experiments and an operator room. Two tests were conducted in parallel, thus four operators (two in the operator room and two in the respective test rooms) had to be present to conduct the study in parallel.

### A. Study Design

At the beginning of the study, participants received a set of instructions including all tasks and questionnaires, as well as an Android device with SIGNAL pre-installed. Each phone (Alice) had a contact entry for the conversation partner (Bob), handled by an operator. The detailed technical setup is described in the next subsection. In the following we describe the tasks participants had to complete as part of our study. The **first part** of the study focused on SIGNAL's general usability related to messaging and security features. In the first task users had to participate in a brief chat conversation with Bob. Bob was simulated by an operator in the operator room. In a second task, participants had to create a password and subsequently export and import a backup of their messages from the first task. With this task we aimed at covering another basic security feature of SIGNAL. In-between the two study parts the MITM attack was initiated by the operator. In the **second part**, participants again had to exchange a few more messages with Bob. Due to the MITM attack of our simulated compromised SIGNAL server, this triggered an error message about Bob's mismatching key (see Figure 3). The task description also asked users to verify Bob's identity, after the message exchange. Our instructions informed participants that they could ask their chat partner Bob into the room at any time. Bob (simulated by an operator) was instructed to play a completely passive role and not to reveal any information on the verification task. Following the verification task, the participants had to fill-in a debriefing questionnaire aimed at assessing the users' mental model of the MITM attack, as well as possible mitigation strategies, by using quantitative and qualitative questions.

### B. Technical Set-Up

In order to conduct our study with two persons in parallel, two identical setups were used which were each administered by one operator. One working setup consists of three smartphones and one computer which was responsible for intercepting the traffic and for creating a WLAN hotspot for the smartphone's internet connectivity. All smartphones were rooted and had Cydia Substrate [15] and SSLTrustKiller [16] installed in order to eliminate the SSL certificate pinning protection of SIGNAL. For traffic interception and manipulation we used mitmproxy [17] in combination with a custom script to automatically intercept SIGNAL messages. Two client smartphones (Android 4.4.4) and one attacker smartphone (Android 4.4.4) were used. The attacker smartphone (Mallory) was preloaded with a modified version of SIGNAL to handle intercepted messages and to forward intercepted messages to the original recipient. The two client smartphones had the latest version of SIGNAL installed (3.15.2). One client smartphone was given to the study participant (Alice), the other client smartphone was used by the operator (Bob) in the operator room. Finally, because all smartphones shared the same network, the smartphones connected to our attack proxy

via a ProxyDroid [18] configuration. For each study participant the devices were reset and re-registered with SIGNAL.

### C. Pilot Study

We conducted a pilot study with six participants from the authors' research groups to refine our study design before the actual study. In our pilot study we asked users to "verify" their communication partner. This request led to confusion as our participants never reached SIGNAL's verification features and had widely diverging understandings of the term "verification". Thus no user successfully managed to compare keys. Based on our results of the pilot study we included a brief explanation of SIGNAL, to point participants towards SIGNAL's technical verification features. Furthermore, we decided to include a "hint": the instructions told the participants that they could ask for their communication partner (Bob) to enter the room at any time. Since participants of the pre-study were unsure whether Bob is a real person or a pre-scripted Bot, this information was crucial to include.

## IV. RESULTS

### A. Participants and general Usability Results

Overall, 28 participants took part in our study (7 female, 21 male), which lasted about 30-45 minutes. All of the participants were computer science students at the University of Vienna, the majority of whom were enrolled in an HCI course and recruited over that course. The only requirement for participation in the study was experience with the Android operating system. The students got a reward in the form of extra points for the HCI course.

Two of the participants were 26-35 years old, the remaining people were in the age between 18 and 25.

Nearly all of the participants actively use text messaging/SMS (27) and WHATSAPP (26) as instant messaging apps, followed by TELEGRAM (18), VIBER (8), FACEBOOK MESSENGER (4) and KAKAOTALK (2). LINE, ANDCHAT, SKYPE, SIGNAL, THREEMA and TANGO were used by one participant each. Regarding self-assessment of computer security knowledge, most of the participants said they had no or some knowledge about privacy and security mechanisms (7 respectively 17), while 4 stated to have a lot of knowledge. None of the participants claimed to be an expert in computer security.

Privacy and security on smartphone apps are of importance to the participants, and they care about third parties reading their messages. Confidentiality of text messages and active security / privacy measures were weighted to be of average importance. Regarding the first usability task (in which participants were asked to exchange a few messages with Bob and send a picture of the lab room), six participants were only partially able to complete the task, since SIGNAL's interface did not indicate whether the image had been send or not. Those pictures were only sent at a later point. All of the other participants were successful. In the second usability task participants were asked to set a passphrase for the app and import/export a backup of the app's data. While setting the passphrase seemed easy, six of the participants were unable to find the backup option. Most of the participants who failed



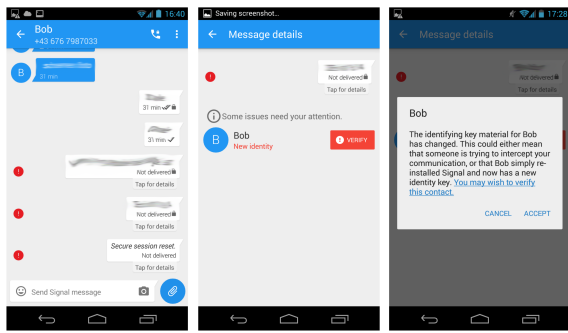


Fig. 3. Message delivery failure (1), notification about Bob’s new identity (2) and new identity dialogue (3)

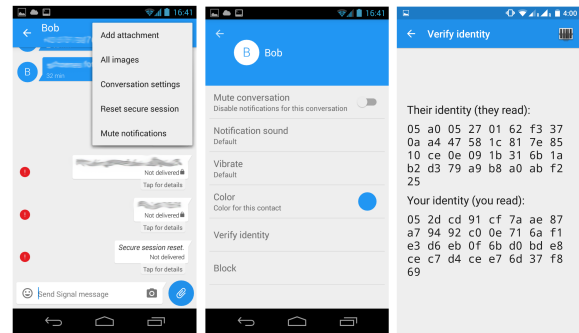


Fig. 4. “Verify identity” option in the conversation settings (1 & 2). Key comparison page displaying Bob’s key at the top and Alice’s resp. the user’s key at the bottom (3).

in this task searched for a backup list item in the preferences section, with the wanted item being located in SIGNAL’s main menu.

### B. Users’ Reactions to the Attack

Shortly before the third task the MITM attack was launched. After the launch of the MITM attack, messages sent through SIGNAL were not delivered since SIGNAL’s protocol needs mutual keys to send messages. In consequence all of the users noticed the attack because of an error notification next to the undelivered message (see Figure 3), and clicked on the notification icon to open the error dialogue.

At this point the error dialogue already confronted the users with the task of verifying Bob. While 24 out of 28 users read the text in the subsequent dialogue, the remaining 4 directly chose the “Accept” option whilst skipping the text. These participants seemed to follow “the flow” of the dialogue to quickly reestablish messaging functionality.

Even if the participants were able to access the key comparison page, whether from the error dialogue or later in the task (8 users never did), the key verification page of SIGNAL’s Android application did not provide any instructions on how to perform the actual verification. As Figure 4 shows (picture on the right), SIGNAL displays the Identity Keys of both communication partners, but no further instructions are provided. The participants of our study therefore faced problems on how to use the displayed keys. One participant e.g. stated: “...ok, those are keys, but what am I gonna do with them?”.

In total 13 users asked Bob into the room during this task for verification, however less than half of those users managed to successfully match keys with Bob (seven users). When keys were correctly compared, a message about verification failure was raised due to the MITM attack (see Figure 2). The error message, however, did not provide any information on consequences, further mitigation strategies or strategy changes. One participant thus said: “Well great, and now what?”, while another participant told us: “To be honest...I have no idea what to do now.”.

### C. Mental Models of the Attack

Ideally, Alice and Bob compare their keys in person for verification purposes to confirm their mutual identity. If Mallory launched a MITM attack on their conversation, Alice and

Bob ideally recognize this type of attack, stop communicating over SIGNAL and uninstall the app. As previously stated, successful MITM attacks on SIGNAL result from their central key exchange services being compromised, Alice and Bob thus need to stop using SIGNAL. In consequence, successful verification of Bob with matching keys was at no point possible in our setup due to the MITM attack. However, 13 participants assumed that they had successfully verified Bob in the final questionnaire, while they failed to correctly compare keys with Bob. They therefore accepted Bob’s new identity and would likely have continued to communicate over an insecure connection since they assumed it to be secure. Those users had different (false) verification strategies, which we discuss in subsection IV-C1. Seven users successfully matched keys with Bob. Only three of those assumed some sort of attack, but did not mention MITM in particular. Two of those users assumed they were not chatting with Bob, but with the attacker Mallory. Three other users thought that the app simply malfunctioned. Thus matching of the keys did not necessarily lead to the correct assumptions. We discuss our participants assumptions below. The rest of the participants (eight users) did not manage to compare keys with Bob and were unsure about having verified Bob or knew they had not. Five of those participants explicitly assumed a MITM attack took place. Subsequently, not all users picked correct mitigation strategies. An overview over strategies users would have chosen is outlined below.

1) *Verification Strategies:* Out of the 13 participants who thought to have verified Bob, but did not manage to do so by comparing the keys, 12 came up with different verification strategies. 6 assumed that accepting Bob’s new key in the error dialogue following the attack successfully verified Bob. 4 “verified” Bob by either meeting him in person or by asking him questions about messages he received and his identity via chat or via phone calls. One person assumed that the presence of the keys on the key comparison page proves the authenticity of Bob’s identity, while another person attempted to verify the authenticity of the chat by asking Bob whether he thought the chat was secure.

2) *Assumptions about the Attack:* In order to assess the users’ assumptions about the attack we included an open question about the “unexpected events” in the final questionnaire. Spoken remarks in the Think Aloud protocol were also taken into account. Overall, 14 participants made remarks about possible explanations for the unforeseen events (multiple mentions

could be made). 7 participants speculated or stated that a MITM attack could have taken place, although only one of those participants compared keys correctly. As already stated not all the participants who successfully compared keys made the right assumptions about the events during the MITM attack. Several other incorrect assumptions were drawn: 4 participants stated that an attacker made an attempt to impersonate Bob, thus they assumed that they had compared keys with Mallory instead of Bob. Furthermore, 3 participants speculated that Bob could have reinstalled SIGNAL as suggested in the error message. Another 3 users assumed that the app was simply malfunctioning. 2 participants finally stated that an attack could have happened, but did not specify the type of attack.

3) *Mitigation Strategies*: The final questionnaire contained another open question about participants' possible mitigation strategies after the unexpected events. The type of attack was deliberately not revealed so as not to bias answers. Also the users' actions and remarks during the last study task were considered. Several possible mitigation strategies (not necessarily referring to MITM attacks in particular) arose from the answers: 11 participants would simply uninstall the app (the only valid mitigation strategy against compromise of the server), although it was not clear whether they wanted to avoid further hassle and would simply use another messaging app, or whether they knew it was the recommended mitigation strategy. Other strategies aimed at gathering more information, such as contacting Bob on another channel via other apps, phone or face-to-face meetings (8 participants), searching for information on the Internet (6 participants) or asking friends (4 participants). 3 participants would inform the developers or read license agreements and policies (3 resp. 1 participants). Another branch of strategies involved problem solving: restarting the app (2 participants), disconnecting the phone from the Internet (2 participants) or a virus scan (1 participant).

## V. DISCUSSION

To the best of our knowledge we are the first to study the security, as well as usability, challenges of end-to-end encrypted messengers. The central services used to exchange user keys pose the major security risk of today's end-to-end encrypted messengers. In our study we therefore simulate a compromised key service by performing an active MITM attack. Hence, we assess the usability of SIGNAL's security features in case of active attacks. However, like any user study, our work has some limitations:

First, the participants recruited for the study were homogeneous since all were students of computer science and shared the same age group. Similar experiments with different groups of participants might therefore lead to different outcomes. Second, we had to balance the extent of information we provided to participants on SIGNAL's encryption/verification features. We decided to explicitly ask users to verify each other in order to assess the usability of this core-security feature of SIGNAL. Our initial study design tested in our pilot study showed that none of the six participants used the verification feature in the face of our simulated attack. Similar experiments with participants without a computer science background and without a focus on a security subtask would likely result in even less successful key verifications. Overall, we were surprised by the outcome of our study,

especially given the fact that our participants had a computer science background. Our results suggest that the "verification" process and therefore the overall security of end-to-end encryption on mobile instant messaging faces serious usability obstacles, since 21 of our 28 participants failed to properly compare keys with their conversational partner. Especially surprising in our study was the high number of participants who thought they had successfully verified while in reality they failed to compare keys.

SIGNAL, as an easy-to-use end-to-end encryption enhanced app, should support struggling users to achieve security in the sense of increased usable security. Usability problems, in terms of missing support, can lead to serious security breaches, e.g. aborting the reestablishment of a secure connection after an attack. The gaps between self-assessment, mental models of differing correctness respectively level of detail as well as actual outcome (un/successful defense) could be explained in several ways: Either participants lacked the required knowledge, the app failed to support the users, they simply had a different understanding of what "verification" meant or the effort for successful defense was simply too high. During the MITM attack, SIGNAL was explicitly hinting at the fact that the connection could have been compromised. The fact that only 7 participants assumed the possibility of a MITM attack and only 3 thought that Bob reinstalled the app seem quite surprising. Either those users ignored, or did not read, the informational error message or simply excluded the possibility of an attack/reinstallation while remaining under the false illusion of security. The different strategies for verification and mitigation definitely hint at flawed mental models: users seem to lack an understanding of end-to-end encryption in general, possible attack scenarios and risk potentials. The findings from section IV-C1 also indicate a great trust by the users in the app to deal with security issues in the background, therefore assuming that the app's dialogues could be trusted.

### A. Recommendations for SIGNAL

We think that SIGNAL can be improved in order to provide end-to-end encryption for the masses and further close the gap between insufficient knowledge on the users' side and possible support through the app. We suggest the following usability improvements to contribute towards an enhanced usable security experience for SIGNAL:

**Awareness on security status of conversations:** Conversations can only be assumed to be properly end-to-end encrypted once Alice's (the user's) and Bob's (the conversational partner's) Identity Keys were successfully verified. SIGNAL does not remember the verification status — only point-in-time verifications are possible and the user has to remember whom of his/her partners he/she already verified. SIGNAL thus lacks mechanisms to quickly assess the security status of a conversation. Such a security status should be directly visible in the corresponding conversation.

**Comprehensible instructions for recommended actions:** In order to avoid risky behavior, especially in the verification and attack mitigation process, users should be provided with clear instructions respectively suggestions for actions. On the key comparison page users with no exact knowledge of asymmetric encryption mechanisms failed to act on the

displayed information. In our opinion, a brief instructional message combined with optional further information would have led to a higher verification success rate (e.g. *“Please contact your partner outside the app to compare your Identity Keys. If the Identity Keys do not match, please consult the FAQ or contact the developers.”*). We found that this issue is most pressing for the Android version of SIGNAL. The iOS version of SIGNAL provides brief information on how to verify users: *“Compare both fingerprints to verify your contact’s identity and the integrity of the message”*. However, no information is provided on how to proceed in case of failure (fingerprint mismatch).

**Clear risk communication:** On the other hand SIGNAL should inform users of the possible consequences of their actions. E.g. during the process of accepting Bob’s identity after the attack the denomination of the buttons (“Verify” and “Accept”) was misleading. Under the false assumption that the mitigation process would lead to a verification of Bob, users failed to have a clear understanding of the risks.

**Easily accessible verification:** The verification options should be easily accessible in the menu. A suggestion would be to add a shortcut for the verification mechanism directly to the conversation in order to maximize visibility.

Based on our findings on the usability of SIGNAL’s error handling of actual attacks, we found that these features led to more problems than to actual attack mitigations. Under these circumstances it is not surprising that WHATSAPP has disabled all encryption related error messages by default. If users want to get feedback on mismatching Identity Keys or alike, they explicitly have to enable the error messages in the preferences. Since reactions to non-comprehensible error messages (due to the interplay of potential missing information on the app’s side and incomplete mental models on the user’s side) range from uninstalling of the app, contacting the developers and/or a definitive feeling of insecurity in general, we assume the developers of WHATSAPP made a compromise between usability and security due to economical reasons. Since communication over WHATSAPP was only encrypted between the client and the server recently, messages on changed Identity Key might lead to confusion, ultimately angry users and eventually uninstallation.

## VI. RELATED WORK

Usable security as relatively new field of research focuses on the development of secure systems including the people who actually use them [19]. Cranor e.g. argues that security failures often originate from unintentional mistakes by users of computer systems due to usability problems [20]. Previous work specifically on the usability of secure messaging focused to a large extend on PGP and S/MIME. A number of experiments showed that this first end-to-end encrypted messaging protocols were plagued with usability issues [1], [2], [3], [4]. These previous results might also explain why PGP and S/MIME have not, as yet, enjoyed widespread adoption. Assal at al. [21] explored mobile privacy through a survey and usability evaluation of three privacy-preserving mobile apps, including the Off-the-Record Messaging application ChatSecure [22]. They observed a high number of participants who thought their conversations were encrypted while they were

not, mainly due to usability issues and incomplete mental models of privacy risks. The study of Assal et al. has a close relation to our work. However SIGNAL communication is encrypted by default and we focus on the unique usability challenges of SIGNAL.

Mental models as an internal representation of concepts have a great influence on cognition, reasoning and decision-making. Although being incomplete and inaccurate by nature, mental models are able to provide predictive and explanatory powers for understanding interaction [23], [24], [25]. Especially with security’s complex problems and concepts, mental models of security or privacy mechanisms and possible threat scenarios play a major role in usable security research. Mental models mediate the processing of risk messages [26]. One possible threat scenario in consequence is for malicious software to take advantage of gaps in the users’ mental models [27]. The same incomplete internal representations of concepts and threats proved to be the reason for low end-to-end encryption uptake, apart from the lack of usability [3]. Nevertheless mental models in usable security research can help to shed light on users’ decisions in case of failure detection [28]. Our work extends research on the use of mental models in the area of usable security and proved helpful to better understand the usability issues our participants faced.

The most comprehensive work on secure messaging has been published by Unger at al. [29]. Their survey provides a current view on challenges for secure messaging, and as such provides additional context for our work especially regarding technical means to verify users and the mitigation of MITM attacks. Regarding the main focus of our work, SIGNAL, Frosch et al. [13] provide a detailed analysis of the underlying cryptographic protocol of SIGNAL. Schrittwieser at al. [30] discuss the different attack vectors like account hijacking, sender ID spoofing, enumeration and several other security issues of early mobile messengers. This study has been complemented by Rottermann et al. [31], who focused on the unique privacy challenges posed by mobile messengers. With the exception of the work by Unger at al. [29], previous work on secure mobile messaging does not discuss usability issues of secure mobile messengers but rather focuses on purely technical issues.

## VII. CONCLUSION

In this paper we presented a user study on the security and usability of SIGNAL for Android, a secure mobile messenger that provides a promising solution for widely adoptable end-to-end encrypted conversations. SIGNAL’s protocol has recently been adopted by WHATSAPP, which means that over one billion users can now potentially exchange messages protected by strong encryption. We first discussed the unique security challenges and threats today’s secure mobile messengers face. Second, we conducted a comprehensive user study on the usability of SIGNAL’s security features. As part of our user study we simulated man-in-the-middle attacks and showed that the great majority of users failed to detect and deter such attacks. We finally proposed a number of improvements for SIGNAL to make the existing security features easier to use.

## REFERENCES

- [1] A. Whitten and J. D. Tygar, "Why johnny can't encrypt: A usability evaluation of ppg 5.0." in *Usenix Security*, vol. 1999, 1999.
- [2] S. L. Garfinkel, D. Margrave, J. I. Schiller, E. Nordlander, and R. C. Miller, "How to make secure email easier to use," in *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM, 2005, pp. 701–710.
- [3] K. Renaud, M. Volkamer, and A. Renkema-Padmos, "Why doesn't jane protect her privacy?" in *Privacy Enhancing Technologies*. Springer, 2014, pp. 244–262.
- [4] A. Fry, S. Chiasson, and A. Somayaji, "Not sealed but delivered: The (un) usability of s/mime today," in *Annual Symposium on Information Assurance and Secure Knowledge Management (ASIA'12)*, Albany, NY, 2012.
- [5] Forbes, "Gartner survey showing declining pcs, increasing mobile devices through 2017," 2013, <http://www.forbes.com/sites/chuckjones/2013/04/05/gartner-survey-showing-declining-pcs-increasing-mobile-devices-through-2017>.
- [6] EFF, "Secure messaging scorecard v 1.0," online, 2015, <https://www.eff.org/node/82654>.
- [7] Open Whisper Systems, "Signal messenger," online, 2016, <https://whispersystems.org>.
- [8] O. W. Systems, "Open whisper systems blog: Just signal," Nov. 2015. [Online]. Available: <https://whispersystems.org/blog/just-signal/>
- [9] The Intercept, "With facebook no longer a secret weapon, egypt's protesters turn to signal," online, April 2016, <https://theintercept.com/2016/04/26/facebook-no-longer-secret-weapon-egypts-protesters-turn-signal/>.
- [10] WhatsApp Inc., "Whatsapp," online, 2016, <https://whatsapp.com>.
- [11] EFF, "Whatsapp rolls out end-to-end encryption to its over one billion users," online, April 2016, <https://www.eff.org/deeplinks/2016/04/whatsapp-rolls-out-end-end-encryption-its-1bn-users>.
- [12] N. Borisov, I. Goldberg, and E. Brewer, "Off-the-record communication, or, why not to use ppg," in *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*. ACM, 2004, pp. 77–84.
- [13] T. Frosch, C. Mainka, C. Bader, F. Bergsma, and T. Holz, "How secure is textsecure?" 2014.
- [14] C. Lewis, *Using the "thinking-aloud" method in cognitive interface design*. IBM TJ Watson Research Center, 1982.
- [15] L. SaurikIT, "Cydia substrate," 2016, <http://www.cydiasubstrate.com>.
- [16] M. Blanchou, "Android-ssl-trustkiller," 2016, <https://github.com/iSECPartners/Android-SSL-TrustKiller>.
- [17] A. Cortesi, "mitmproxy," 2016, <https://mitmproxy.org/>.
- [18] M. Lv, "Proxydroid," 2016, <https://github.com/madeye/proxydroid>.
- [19] L. F. Cranor and S. Garfinkel, *Security and usability: designing secure systems that people can use*. O'Reilly Media, Inc., 2005.
- [20] L. F. Cranor, "A framework for reasoning about the human in the loop." *UPSEC*, vol. 8, pp. 1–15, 2008.
- [21] H. Assal, S. Hurtado, A. Imran, and S. Chiasson, "What's the deal with privacy apps?: a comprehensive exploration of user perception and usability," in *Proceedings of the 14th International Conference on Mobile and Ubiquitous Multimedia*. ACM, 2015, pp. 25–36.
- [22] C. Ballinger, "Chatsecure - encrypted messenger for ios and android," online, 2016, <https://chatsecure.org>.
- [23] P. N. Johnson-Laird, *Mental models: Towards a cognitive science of language, inference, and consciousness*. Harvard University Press, 1983, no. 6.
- [24] N. Staggars and A. F. Norcio, "Mental models: concepts for human-computer interaction research," *International Journal of Man-machine studies*, vol. 38, no. 4, pp. 587–605, 1993.
- [25] N. Jones, H. Ross, T. Lynam, P. Perez, and A. Leitch, "Mental models: an interdisciplinary synthesis of theory and methods," 2011.
- [26] L. J. Camp, "Mental models of privacy and security," *Available at SSRN 922735*, 2006.
- [27] R. Wash, "Folk models of home computer security," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM, 2010, p. 11.
- [28] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri, "Bridging the gap in computer security warnings: A mental model approach," *IEEE Security & Privacy*, no. 2, pp. 18–26, 2010.
- [29] N. Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg, and M. Smith, "Sok: Secure messaging," in *Security and Privacy (SP), 2015 IEEE Symposium on*. IEEE, 2015, pp. 232–249.
- [30] S. Schrittwieser, P. Frühwirth, P. Kieseberg, M. Leithner, M. Mulazzani, M. Huber, and E. R. Weippl, "Guess who's texting you? evaluating the security of smartphone messaging applications." in *NDSS*, 2012.
- [31] C. Rottermann, P. Kieseberg, M. Huber, M. Schmiedecker, and S. Schrittwieser, "Privacy and data protection in smartphone messengers," 2015.

# Users Protect Their Privacy If They Can: Determinants of Webcam Covering Behavior

Dominique Machuletz\*, Henrik Sendt†, Stefan Laube‡ and Rainer Böhme<sup>x</sup>

\*†‡*Department of Information Systems, Westfälische Wilhelms-Universität Münster, Germany*  
Email: \*D.Machuletz@uni-muenster.de, †H.S@uni-muenster.de, ‡ Stefan.Laube@uni-muenster.de

<sup>x</sup>*Department of Computer Science, Universität Innsbruck, Austria*  
Email: Rainer.Boehme@uibk.ac.at

**Abstract**—Most notebooks sold today come with a built-in webcam, placed above the screen to facilitate users’ visual communication. What is intended to be a service seems to raise privacy concerns to some users, who may seek protection by covering the webcams of their devices. No matter how effective, this habit makes users’ actual privacy protection behavior observable to researchers. This paper presents an application of the Theory of Reasoned Action to investigate determinants that lead users to cover their notebook webcams. It is based on an analysis of face-to-face interview data collected from 113 individuals who used their notebooks in public places, e. g., libraries, cafés, or trains. These users self-reported their attitudes and subjective norms towards webcam covers and privacy in general, while the actual covering behavior was observed and recorded by the interviewer. We estimate three logistic regression models to analyze the data. Our results indicate that attitudes towards webcam covers can explain actual covering behavior. Furthermore, we do not observe that participants’ attitudes or subjective norms towards privacy have a manifest impact on the behavior.

**Index Terms**—Privacy, Usability, Actual Protection Behavior, Webcam Cover, Theory of Reasoned Action, Field Study

## 1. Introduction

Undoubtedly, recent advances in information technology reduce users’ actual and perceived control over their personal data [1]. Consequently, concerns about information privacy are rising [2]. Information privacy refers to “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” [3]. Hence, it is about the

decision to transfer personal data to third parties. This decision was easy to make during the early stages of the digital revolution. At that time, data generating sensors in personal devices barely existed, and users had almost full control over the information stored in memories. Furthermore, the technical capabilities of vendors were limited, such that it was not easy for them to transfer and analyze mass data recorded by their products [4]. Today, users’ devices have the capability to collect big quantities of personal data and send it into “the cloud” at negligible cost [2]. Furthermore, user-facing cybercrime [5] and mass data analysis by businesses [6] and governments are hot topics. If devices collect and distribute users’ personal data without their explicit consent to others, we speak of privacy violations. Many users are concerned about such violations [7]. This motivates research on users’ privacy protection behavior.

Several studies on users’ privacy protection behavior use varying research methods. Some scholars try to investigate behavior based on self-reported data collected with questionnaires (e. g., [8], [9], [10]). However, the reliability of these results is limited, as self-reports may not always reflect actual user behavior [11]. This has led to a string of privacy studies that focus on privacy measures disclosed by users in laboratory experiments (e. g., [12], [13], [14]). The weakness of these studies is that the experimental setting may bias participants’ behavior. Besides the well-known Hawthorne effect [15], privacy experiments face the particular difficulty of creating a credible stimulus for the risks of data sharing without crossing ethical boundaries. This motivates research on users’ self-disclosed privacy protection behavior in public (e. g., [16], [17], [18]).

In the tradition of these latter studies, we investigate factors that lead users to cover their notebook lenses with a piece of tape or dedicated covers. Webcam covers are simple, user-understandable “mechanism” reducing the risk of falling victim to webcam spying attacks. According to a report published in June 2015 [19], they are commonly used among Internet users worldwide. As today’s technological infrastructure enables users to access the Internet with notebooks from almost everywhere in the world, covering behavior must be observable at public places. This motivates us to conduct a study where we assess notebook webcam covering behavior of users at public places, coupled with a questionnaire to measure personal characteristics leading to

Permission to freely reproduce all or part of this paper for noncommercial purposes is granted provided that copies bear this notice and the full citation on the first page. Reproduction for commercial purposes is strictly prohibited without the prior written consent of the Internet Society, the first-named author (for reproduction of an entire paper only), and the author’s employer if the paper was prepared within the scope of employment.

EuroUSEC ’16, 18 July 2016, Darmstadt, Germany  
Copyright 2016 Internet Society, ISBN 1-891562-45-2  
<http://dx.doi.org/10.14722/eurousec.2016.23014>

this behavior. To the best of our knowledge, our study is the first to causally investigate webcam covering behavior.

The rest of this paper is structured as follows. We discuss relations of our approach to prior art and propose our research question in Section 2. Section 3 introduces our research method. We conduct our analysis in Section 4, and present its results in Section 5. A discussion of the results and study limitations in Section 6 precedes our conclusion in Section 7.

## 2. Related Work and Research Question

Scholars have investigated for long the relationship between users' privacy preferences and actual privacy protecting behavior. We briefly review prominent studies related to our work in Section 2.1. Thereafter, in Section 2.2, we put our approach to measure webcam covering behavior into context and derive our research model. The availability of data to apply this research model is conditioned on users' perceived risk of uncovered webcams, which we examine in Section 2.3. However, this risk may vary between users, motivating our research question proposed in Section 2.4.

### 2.1. Privacy Preferences vs. Actual Behavior

Many studies reveal discrepancies between users' privacy preferences and their actual privacy protection behavior. This is commonly referred to as the *privacy paradox*, a term defined by Norberg *et al.* [20] as "the difference between information actually provided [by users] as compared to a willingness to provide."

Diverse studies on users' privacy preferences and actual behavior on the Internet present evidence for the existence of a privacy paradox. All of these studies stand in the tradition of work by Spiekermann *et al.* [12], who conduct an experimental study to reason about the relationship between users' privacy preferences and disclosure behavior during online shopping. Their results indicate that many users disclose a lot of personal information regardless of their self-reported privacy concerns. Following the central idea proposed in [12], other scholars conduct similar studies, experimenting in scope. For instance, Tufekci [21] analyzes the relationship between privacy concerns and disclosing behavior of *Facebook* and *Myspace* users. They find that users' general online privacy concerns do not influence their information disclosure on online social networking sites. The studies in [22], [23], [24] yield similar results.

Other studies refute the hypothesis that there is a privacy paradox. For instance, the authors of [25], [26], [27], [28], [29], [30] all find correlations between social network users' privacy concerns and their behavior to introduce strict privacy settings. Dinev and Hart [10] analyze factors that influence users' information disclosure on online shopping websites. They find that a high level of perceived Internet privacy risk relates to a low willingness to provide personal information. Similarly, George [9] examines the relationship between users' purchasing behavior on the Internet and their privacy concerns when transacting with merchants. His work reveals that when users believe in the Internet's

trustworthiness and their own ability to buy online, they are more likely to transact with merchants than those without these characteristics. Finally, one could argue that there is no paradox at all because stated attitudes are generally a weak predictor of actual behavior; even more so as many privacy studies do not strictly observe the "principle of compatibility" (see [31], [32], [33]) in their measurements.

### 2.2. Theoretical Classification and Research Model

Our study on webcam covering relates to the works presented in the previous section as it adopts commonly used constructs: users' attitudes and subjective norms towards privacy protection behavior. Attitudes towards a behavior reflect the degree to which a user has a favorable or unfavorable evaluation of the behavior. Subjective norms reflect the perceived social pressure to perform (or not to perform) the behavior in question [31].

The Theory of Reasoned Action (TRA) [34] and the Theory of Planned Behavior (TPB) [31] position both constructs in a broader context. The theories have in common that they assume users' attitudes and subjective norms to affect behavioral intention, influencing actual behavior. Their main difference is that the TPB adds the user's perceived behavioral control as a construct. Hence, the application of the TPB is reasonable when the behavior of interest is not under complete volitional control [32]. In contrast, the TRA is appropriate to analyze behavior that can fully be determined by users. A premise of our research is that webcam covering is under full volitional control of users and does not require specific skills or knowledge. Thus, we choose the TRA as the theoretical basis for our work.

Our research model for this study, based on the TRA, is depicted in Fig. 1. It comprises two constructs: attitudes towards privacy and webcam covers; and subjective norms towards privacy and webcam covers. We can neglect the intention construct provided for in the original TRA, as its measurement does not have a predictive value: the intention construct is dispensable if data on users' intentions and actual behavior are collected simultaneously (see [9], [35], [36]). Thus, in our model users' attitudes and subjective norms directly influence webcam covering.

In order to be able to apply our research model, we require data on users' covering behavior. Such behavior is conditioned on perceived risk of uncovered webcams.

### 2.3. Risk of Uncovered Webcams

Users seem to perceive a risk of webcam misuse, although the actual risk is deemed rather small. Webcam spying is usually enabled by users themselves, who unintentionally download and install a remote administration tools (RAT) on their devices. Prominent examples of these tools are the "Blackshades" malware and the spyware "Dark-Comet". Once a tool is installed, it can be exploited by the attackers who initially disseminated them. There are reported cases for *private hackers* using these tools in order

to spy on users.<sup>1</sup> Additionally, it is conceivable that *firms* are actively involved in webcam spying, e.g., on their employees.<sup>2</sup> Moreover, there are indicators that *government agencies*, e.g., the US Federal Bureau of Investigation (FBI), circulate RATs in order to spy on their citizens.<sup>3</sup> In fact, the FBI Director’s own use of a webcam cover indicates that spying on webcams may be a persistent threat.<sup>4</sup> However, we are not aware of any scientific evidence for real attacks. Overall, the privacy risk to consumers arising from uncovered webcams might be negligible compared to, e.g., browser-based network tracking as investigated in [37]. Nevertheless, users seem to perceive the small risk of webcam spying. For instance, this is confirmed by a study of Portnoff *et al.* [38], assessing the effectiveness of webcam indicator lights in communicating a webcam’s recording to users by conducting a laboratory experiment. Among other things, they find that the majority of their study participants recognize the possibility of webcam spying attacks. Most of them would immediately cover their webcam if it unexpectedly indicated recording. However, users’ perceived risk of uncovered webcams may vary. This motivates a privacy study on determinants that lead users to cover their webcams.

## 2.4. Research Question

The overall research question in this paper is:

*“Which personal characteristics influence users’ behavior to cover their notebook webcams?”*

This question can be refined using the following two hypotheses that relate to our research model in Figure 1:

- H1 Attitudes towards webcam covers and privacy significantly affect webcam covering behavior.
- H2 Subjective norms towards webcam covers and privacy significantly affect webcam covering behavior.

## 3. Method

In order to answer the research question and to test the proposed hypotheses, we collected data by conducting a survey and observing participants’ webcam covering behavior. We present the survey instrument in Section 3.1 and describe our survey procedure in Section 3.2.

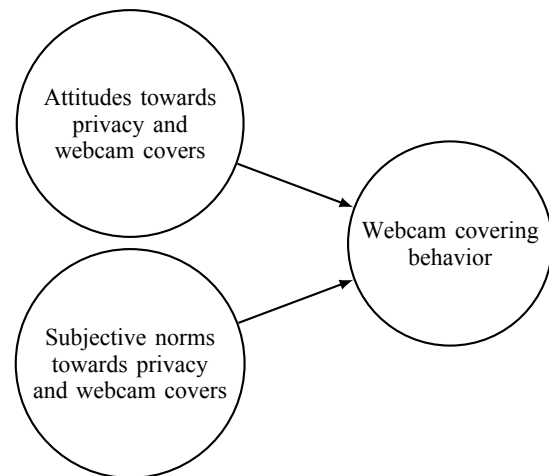
1. See, e.g., <http://www.bbc.com/news/technology-34475151> and <http://stoplooking.net/how-the-fbi-found-miss-teen-usas-webcam-spy/>.

2. This is, for instance, mentioned in [http://www.huffingtonpost.com/rebecca-abrahams/your-computer--phone-came\\_b\\_5398896.html](http://www.huffingtonpost.com/rebecca-abrahams/your-computer--phone-came_b_5398896.html).

3. See <http://www.dailymail.co.uk/news/article-2520707/FBI-spy-webcam-triggering-indicator-light.html> for further information.

4. During a speech in Ohio, USA, FBI Director James Comey pointed out that he uses a webcam covers on his own laptop. See <https://nakedsecurity.sophos.com/2016/04/12/why-the-fbi-director-puts-tape-over-his-webcam-and-you-should-too/>.

Figure 1. Research Model Based on the TRA



### 3.1. Instrument

Our instrument is designed to measure one dependent and two independent variables. The measurement of the dependent variable is presented in Section 3.1.1. Thereafter, in Section 3.1.2, we introduce the measurement and reliability scores of the two independent variables.

**3.1.1. Dependent Variable.** Webcam covering behavior is the dependent variable in our model. This variable does not have to be reported by participants, but is unobtrusively observed by the interviewer once users agree to participate in the study.

**3.1.2. Independent Variables.** The study’s two independent variables concern participants’ attitudes and subjective norms. Both have to be self-reported by participants. They are regarded as constructs measured *reflectively* with multiple items on seven-point rating scales, anchored at 1 (fully disagree) and 7 (fully agree). The measurement of all items is performed in German, with original wording reported in Table 5 (in the Appendix).

The attitudes construct consists of 12 items (Cronbach’s  $\alpha = 0.76$ ). We use 7 items for measuring attitudes towards webcam covers (Cronbach’s  $\alpha = 0.84$ ), asking participants about their subjective perceptions and opinions that relate to this privacy protecting behavior. Furthermore, 5 items are used to measure attitudes towards privacy (Cronbach’s  $\alpha = 0.46$ ), focusing on personal beliefs and perceptions regarding privacy preserving behavior, as well as opinions about privacy related topics.

The subjective norms construct consists of 8 items (Cronbach’s  $\alpha = 0.44$ ). We use 4 items to measure subjective norms towards webcam covers (Cronbach’s  $\alpha = 0.52$ ). Related questions ask for participants’ perceptions how their social environment regards webcam covering. Moreover, we use 4 items for measuring subjective norms towards privacy (Cronbach’s  $\alpha = 0.37$ ), investigating participants’ perceptions on how others regard information privacy.



### 3.2. Procedure

Our data collection took place in October 2015. We interviewed users of notebooks with webcams at different libraries, trains, canteens and cafés in and around Münster, a college town in Germany. Everyone who used a notebook with a webcam in public has been considered a potential study participant. We asked candidates whether they would like to take part in a research project dealing with notebook usage behavior. In this context, we informed them about the expected duration as well as the voluntary nature of participation in our study. Furthermore, we guaranteed anonymity. Once a candidate agreed, we handed out our survey on paper and secretly recorded his webcam covering behavior. On average, it took study participants about 4–5 minutes to complete the questionnaire. Subjects were debriefed after they took the survey. This included informing them on our recordance of webcam covering behavior.

### 4. Analysis

Our data analysis is based on  $n = 113$  study participants. Their demographics, depicted in Table 1, are presented in Section 4.1. Thereafter, in Section 4.2, we propose the statistical model used to analyze the data.

#### 4.1. Descriptive Analysis

By discussing the survey demographics we can give some intuition on how widespread the use of webcam covers is among different groups of study participants.

In total, 32% of all participants had a webcam cover.

Our sample contains more male (61%) than female (37%) participants, and is biased towards people aged between 18 and 29 (81%). One reason for this bias may be that the town where the data has been collected is small in comparison to its number of students.<sup>5</sup>

Of all female participants, we observe that nearly half had a webcam cover (43%). By contrast, only about one quarter (26%) of all males covered their webcams. We use Pearson’s chi-squared test to assess differences between these two groups. The hypothesis that webcam covering behavior is independent of gender can be rejected with a significance level of 10% ( $\chi^2 = 3.35$ ,  $df = 1$ ,  $p = 0.067$ ).

Of all young participants, about one third (32%) covered their webcam. We assume that younger people are in general more likely to cover their webcams than older ones. This is because younger generations grow up using information technology, and thus might develop an instinct regarding threats to their devices. Though, we cannot evaluate this assumption as the remaining age groups in our sample are too small to statistically test differences in webcam covering customs.

The demographics suggest that a considerable amount of participants (12%) make use of webcam covers even though

5. In the most recent demographics of Münster from 2014, the town had about 300,000 residents. Simultaneously, about 45,000 students were registered at the local university.

Table 1. Survey Demographics

	Frequency (#)	Of all (%)	With cover (%)
<b>Total</b>	113	100.0	31.9
<i>Gender</i>			
Male	69	61.1	26.1
Female	42	37.2	42.9
Unknown	1	0.9	0.00
<i>Age</i>			
< 18	6	5.3	33.3
18 – 29	92	81.4	31.5
30 – 39	4	3.5	50.0
40 – 49	2	1.8	50.0
50 – 59	9	8.0	22.2
> 59	0	0.0	0.0
<i>Notebook usage per day (hours)</i>			
< 1	17	15.0	11.8
1 – 2	24	21.2	29.2
3 – 4	27	23.9	44.4
5 – 6	13	11.5	38.5
> 6	31	27.4	32.3
<i>Webcam usage during last month (times)</i>			
0	63	55.8	31.8
1 – 4	38	33.6	26.3
5 – 8	5	4.4	80.0
> 8	7	6.2	28.6
<i>Antivirus installed</i>			
Yes	98	86.7	31.6
No	15	13.3	33.3
<i>Mobile phone front camera covered</i>			
Yes	3	2.7	66.7
No	103	91.2	28.2
<i>Use of mobile phone privacy filter</i>			
Yes	7	6.2	57.1
No	103	91.2	31.1

Some variables have missing values.

they use their notebook for less than one hour a day. If participants indicate to have the habit of using their notebooks for longer than one hour a day, they are more likely to make use of webcam covers. Specifically, about a third of these participant (36%) covered their webcam on average. We use Pearson’s chi-squared test to assess behavioral differences between the two notebook usage types. The hypothesis that webcam covering behavior is independent of notebook usage per day can be rejected with a significance level of 5% ( $\chi^2 = 3.82$ ,  $df = 1$ ,  $p = 0.050$ ). An explanation may be that participants who use their notebook more frequently are better informed about potential risks, and therefore more likely to take precautionary measures.

In total, the majority of participants in our sample (56%) reported that they did not use their webcams at all during the past month. Nevertheless, about one third of these participants (32%) uses a webcam cover, regardless. However, based on our data, a causal link between the frequency of webcam usage and webcam covering behavior cannot be established.

Additionally, we can investigate relationships between participants’ webcam covering behavior and their use of other security or privacy measures. We cannot find any correlation between covering behavior and used security measures, such as antivirus software. Furthermore, of all participants with a webcam cover in place (32%), most

Table 2. Regression with All Items

Item code	Item description	Estimate	Exp. Estimate	Std. error	z value	Pr(> z )
(Intercept)		-5.76	0.00	3.89	-1.48	0.138
<i>Attitudes towards webcam covers</i>						
AW1	Fear of unauthorized webcam access	1.52	4.57	2.29	0.66	0.507
AW2	Opinion that one should protect from unauthorized webcam access	-2.45	0.09	2.33	-1.05	0.294
↔AW3	Perception that webcam covering is excessively cautious	0.12	1.12	2.28	0.05	0.960
<b>AW4</b>	<b>Perception that webcam covers are practical</b>	5.32	204.24	2.12	2.51	0.012 *
AW5	Perception that webcam covers are useful	-0.82	0.44	3.23	-0.25	0.800
<b>AW6</b>	<b>Perception that webcam covers are necessary</b>	7.18	1311.15	2.30	3.13	0.002 **
AW7	Perception that webcam covers are secure	1.04	2.82	2.24	0.46	0.643
<i>Attitudes towards privacy</i>						
↔AP1	Opinion that video cameras should be used at public places to increase security	-0.28	0.75	2.14	-0.13	0.895
↔AP2	Perception that the disclosure of own personal information in social networks is harmless	-3.25	0.04	2.91	-1.12	0.264
↔AP3	Willingness to upload a personal video on a public website	-0.85	0.43	2.52	-0.34	0.737
↔AP4	<b>Belief that the government sufficiently protects personal privacy on the Internet</b>	-6.31	0.00	3.18	-1.99	0.047 *
↔AP5	<b>Belief that firms respect personal privacy</b>	4.91	135.80	2.31	2.12	0.034 *
<i>Subjective norms towards webcam covers</i>						
<b>SW1</b>	<b>People in the social environment use a webcam cover</b>	-7.63	0.00	3.24	-2.35	0.019 *
<b>SW2</b>	<b>People in the social environment argue for webcam covering</b>	10.23	27758.95	3.90	2.62	0.009 **
SW3	Expectation of others to use a webcam cover in the work environment	2.70	14.89	2.12	1.27	0.203
↔SW4	Fear that others rate webcam covering overly cautious	-0.83	0.43	2.42	-0.34	0.731
<i>Subjective norms towards privacy</i>						
SP1	Perception that society expects Internet privacy self-protection	-3.45	0.03	1.87	-1.84	0.065
SP2	Privacy protection is an important topic in the social environment	1.01	2.76	2.02	0.50	0.614
↔SP3	Fear of social rejection for not being active in social networks	1.73	5.65	2.42	0.72	0.474
↔SP4	Fear of social rejection for not sharing pictures in social networks	-6.26	0.00	4.08	-1.54	0.125

Scales of items indicated by “↔” were reversed before conducting the analyses in Section 5.2 and Section 5.3

Significance level codes: 1% ‘\*\*\*’, 5% ‘\*’

Nagelkerkes’ pseudo- $R^2 = 0.74$

did not cover their mobile phone front camera (88%). By contrast, of all participants who indicated to cover their mobile phone front camera (3%), most had a webcam cover in place (67%). We also asked all participants if they use mobile phone privacy filters. Of the few study participants who used filters (6%), a considerable share (57%) also covered their notebook webcam.

We closed our questionnaire with two open questions. First, we asked participants with a webcam cover in place for how long they have been covering. Most of them (75%) answered that they cover their webcam for longer than one year. Second, we asked participants without a webcam cover regarding their covering behavior in the past. Surprisingly, some participants (17%) revealed that they once used a cover. A considerable amount of these participants (62%) stated a loss of the cover or the purchase of a new notebook as reasons for a change in behavior. Others (38%) mentioned that impracticability or poor outer appearance of webcam covers lead them to discontinue covering.

## 4.2. General Statistical Model

For an investigation of the relation between our independent and dependent variables, we compute logistic regressions. This is possible because our dependent variable is binary (webcam covered/not covered) and the independent

variables are based on parametric measures. Thus, we may estimate the parameter vector  $\hat{b} = (\hat{b}_0, \hat{b}_1, \dots)$  using the following equation per response record to derive results considering all items:

$$\log\left(\frac{p}{1-p}\right) = \overbrace{b_0 + b_1 D_1 + \dots}^{\text{Behavior}} + \overbrace{b_2 D_2 + \dots}^{\text{Attitudes}} + \overbrace{b_i D_i + \dots}^{\text{Subjective norms}} + \epsilon,$$

where

- the dependent variable  $p$  is the probability for a participant to use a webcam cover,
- $b_0$  is a constant intercept,
- $(D_1, \dots, D_{i-1})$  are values derived from questions on the participant’s attitudes,
- $(D_i, \dots)$  are values derived from questions on the participant’s subjective norms,
- and  $\epsilon$  is an error term reporting the difference between the true relationship and the model.

However, not every participant answered all questions. Thus, we need to handle missing values before conducting our analyses. We use the policy to discard response records from the data set if more than two values are missing. Otherwise, we fill in missing values by mean value imputation. Overall, our data set includes 22 records with missing

values. Of these records, 13 are deleted based on our policy. Consequently, means are imputed for missing values in the other 9 records. Descriptive statistics for the influence of specific indicators based on the remaining  $n = 100$  data records are provided in Table 6 (in the Appendix). This set of data records is used to compute our regression results. In order to estimate  $\hat{b}$  with the maximum likelihood method, we use the implementation provided by the survey extension for R [39].

## 5. Results

We present results derived by the general statistical model in Section 5.1. This model can be adopted to two aggregate models, whose analysis enables us to reason on the impact of participants’ overall attitudes and subjective norms. Corresponding adoptions and results are presented in Section 5.2 and Section 5.3. Tables 2–4 display the estimated coefficients  $\hat{b}$  along with the exponentiated coefficients  $e^{\hat{b}}$ , standard errors,  $z$ -statistics, associated  $p$ -values and significance levels of the three different models. Each presented coefficient provides an indicator for the impact of a change in the log odds ratio of the dependent variable. Note that only the sign and magnitude of logistic regressions’ coefficients can readily be interpreted, while actual values are not always intuitive. A positive coefficient denotes that – after controlling for all other variables in the model – an answer to the item within the upper half of the rating scale increases the likelihood of notebook webcam covering, and vice versa.

### 5.1. Regression with All Items

Table 2 depicts the results for the statistical model presented in Section 4.2. Our model specification explains about 74% of the variation in the dependent variable.

We observe three characteristics that have a significant and positive impact on participants’ webcam covering behavior. First, participants’ perception that webcam covers are practical (AW4) leads them towards covering their webcam. This finding goes in line with answers to the second of our open-ended questions in the questionnaire: impracticability is one of the reported reasons for participants to stop using webcam covers. Second, participants’ perception that webcam covers are necessary (AW6) has a positive impact on covering behavior. As we did not ask for the root causes of this perception, we may assume that necessity is perceived because of (reports of) experiences with webcam hacks in the past. Another explanation could be social pressure. This would go in line with our third observation: if people in the social environment of a participant argue for the use of webcam covers (SW2), this has a positive impact on behavior adoption.

However, this last result lets another finding appear to be puzzling: participants’ observation that others in their social environment use webcam covers (SW1) has a significant and negative impact on the adoption of this behavior. A quick look at the descriptive statistics in Table 6 (in the

Table 3. Regression with Items Condensed to Four Variables

	Estimate	Exp. Estimate	Std. Error	$z$ value	Pr(>  $z$  )
(Intercept)	-9.49	0.00	2.55	-3.72	0.000 ***
<b>Attitudes towards webcam covers</b>	7.20	1343.99	1.86	3.86	0.000 ***
Attitudes towards privacy	3.02	20.49	2.38	1.27	0.205
Subjective norms towards webcam covers	3.41	30.12	1.87	1.82	0.068
Subjective norms towards privacy	-0.11	0.90	1.82	-0.06	0.952

Significance level code: 0.1% '\*\*\*\*'  
Nagelkerkes’ pseudo- $R^2 = 0.46$

Appendix) reveals that the sign of the estimated coefficient of SW1 points in the opposite direction as suggested by the difference in means. This indicates a suppression effect [40]. In fact, if the logistic regression is computed based on the general model but omitting SW2, we find that SW1 becomes insignificant. Thus, SW1 is suppressed by SW2. This indicates that webcam covers are issues discussed in the social environment of some participants. Moreover, partisanship for and actual use of webcam covers are obviously not independent.

Furthermore, we observe one characteristic that leads participants to abstain from webcam covering. Our results show that participants’ belief that governments sufficiently protects their Internet privacy (AP4) has a significant and negative impact on webcam covering behavior. This result is intuitive and pronounces the role of governments regarding users’ privacy protection.

By contrast to the previous result, participants’ belief that firms respect personal privacy (AP5) has a positive impact on behavior adoption. This result is somewhat surprising, as webcam covering indicates distrust. Table 6 (in the Appendix) reveals that the estimated coefficient of AP5 points in the opposite direction as suggested by the descriptives, signaling a second suppression effect. A closer investigation reveals that AP4 suppresses AP5. A logistic regression computed omitting AP4 lets AP5 become insignificant. This may indicate that some webcam users differentiate between threats and the specific effectiveness of webcam covers: those who cover their lenses mainly for distrust against government spies may be aware that this behavior is of little help against commercial tracking.

Overall, the observed suppression effects indicate that our instrument should be refined in follow-up studies, e. g., by adding more direct items on the perceived effectiveness of webcam covers against specific threats, or by exploring the role of visible covers on personal devices as political statements. Future studies should also include a wider range of questions about trust/distrust in other types of possible attackers (e. g. relating to private attackers).

## 5.2. Regression with Four Variables

In this section, we estimate the parameter vector  $\hat{b} = (\hat{b}_0, \hat{b}_1, \hat{b}_2, \hat{b}_3, \hat{b}_4)$  after we condense all data items to four variables ( $\bar{D}_1, \bar{D}_2, \bar{D}_3, \bar{D}_4$ ): attitudes towards webcam covers, attitudes towards privacy, subjective norms towards webcam covers, and subjective norms towards privacy. Note that we have to reverse some item scales (depicted by a “ $\leftrightarrow$ ” in Table 2) to derive meaningful mean values. For instance, the scaling of the item “API Opinion that video cameras should be used at public places to increase security” has to be reversed as answers in the lower rather than the upper half of the rating scale indicate attitudes towards privacy. After computing the regression results, we are able to reason which of the four variables can best explain webcam covering behavior.

This model specification explains 46% of the variation in the dependent variable, as depicted in Table 3. We observe that only attitudes towards webcam covers have a strong and significant positive impact on webcam covering behavior. Attitudes towards privacy and subjective norms do not predict behavior at all. Thus we cannot confirm that privacy aware participants are likely to cover their webcams, or society at large has an impact on this behavior.

## 5.3. Regression with Two Variables

We may also estimate the parameter vector  $\hat{b} = (\hat{b}_0, \hat{b}_1, \hat{b}_2)$  after we condense all item data to two variables ( $\bar{D}_1, \bar{D}_2$ ): attitudes towards webcam covers and privacy, and subjective norms towards webcam covers and privacy. Again, we have to reverse some item scales to conduct a meaningful analysis, following the rationale proposed in the last Section. The resulting  $\hat{b}$ , derived by the maximum likelihood method, enable us to answer our hypotheses posed in Section 2.4.

This model specification explains 43% of the variation in the dependent variable, as depicted in Table 4. The regression results indicate that attitudes towards webcam covers and privacy have a strong and significant positive impact on webcam covering behavior. In contrast, subjective norms do not predict the behavior at all.

## 6. Discussion

After analyzing the data and reporting of associated results, we can now revisit the hypotheses proposed in Section 2.4.

- H1 *Supported for attitudes towards webcam covers*  
H2 *Not supported*

Regarding H1, we find that participants with an attitudes towards webcam covers and privacy are more likely to use a notebook webcam cover than others. Based on our regression analyses, we can conclude that predominantly attitudes towards webcam covers have a positive impact on behavior. Specifically, participants’ perceived practicability and necessity of covers leads them to adapt covering behavior.

Table 4. Regression with Items Condensed to Two Variables

	Estimate	Exp. Estimate	Std. Error	z value	Pr(> z )
(Intercept)	-11.05	0.00	2.37	-4.66	0.000 ***
<b>Attitudes towards webcam covers and privacy</b>	11.82	135537.01	2.89	4.09	0.000 ***
Subjective norms towards webcam covers and privacy	3.39	29.78	2.53	1.34	0.180

Significance level code: 0.1% \*\*\*\*

Nagelkerkes’ pseudo- $R^2 = 0.43$

Contrary to our expectation, the results also indicate mixed findings on whether privacy preferences have a significant and positive impact on webcam covering.

With respect to H2, we do not find evidence that subjective norms towards webcam covers and privacy significantly affect covering behavior. This may be explained by the low internal consistency of the corresponding items. Acknowledging the results in Section 5.1, we find that participants’ behavior is influenced by people in their social environment who use a webcam cover and argue for it.

In general, we observe that females cover their webcams more often than males, and that covering behavior depends on users’ notebook usage per day. Future research should strive to rule out the potential effect of third variables driving these headline results. No causal relationship can be found between covering behavior and the frequency of webcam usage or the use of notebook security measures.

Our study has a number of limitations. First, we have a selection bias. Our recruitment procedure seeks interviews with users who use notebooks in public only, excluding those who use their devices at home or at work. Those are environments where the expectation of privacy might be even higher and people may use different devices. Second, some reliability scores of our questionnaire are rather weak, as discussed in Section 3.1. Third, our models in Section 5.2 and Section 5.3 have a fairly weak fit. Because of these last two limitations, the corresponding results have to be interpreted with caution. In general, we suggest that future investigations also take different constructs into consideration and refine the item batteries in the questionnaire. We see considerable potential for further research on webcam covering behavior and consider this work a preliminary study, mainly to explore and structure the use of a novel and interesting indicator of actual privacy protection behavior.

## 7. Conclusion

Portable devices with integrated webcams bring numerous benefits to users. They are convenient to use, enable face-to-face communication over the Internet, serve as barcode scanners, etc. Unfortunately, these devices also raise privacy concerns. This is because cybercriminals can hijack

them and blackmail victims with obtained footage, vendors may collect data via the devices for their own economic advantage, and governments can take over webcams as part of their missions to combat organized crime and terrorism. Thus, many users choose to forgo some of the benefits of webcams and cover their notebook lenses with a piece of tape or even dedicated covers available on the market.

To the best of our knowledge, we present the first empirical analysis that tries to shed light into users' webcam covering behavior. Our results indicate that attitudes towards webcam covers have a positive impact on the use of covers. Specifically, participants who perceive covers as necessary or practical adopt this behavior. Furthermore, we do not find evidence that attitudes or subjective norms towards privacy have a measurable impact on covering behavior.

More than 30% of the participants of our convenience sample do use a webcam cover. This not only provides a useful indicator of actual privacy protection behavior for empirical research. It also gives rise to optimism that users take action to protect their privacy

- if the measure is simple,
- perceived as effective,
- and socially acceptable.

Developers of privacy enhancing technologies (PETs) should take this as a lesson on the value of usability. They should try to copy the success factors of this hardware gadget to the truly effective software-based protection mechanisms they design.

## Acknowledgments

The authors acknowledge the help of Severin Hußmann and Hanno Jenkel in collecting the survey data and for their contributions to the data analysis. Furthermore, they thank all study participants for their time.

## References

- [1] E. A. Whitley, "Informational privacy, consent and the 'control' of personal data," *Information Security Technical Report*, vol. 14, no. 3, pp. 154–159, 2009.
- [2] J. van den Hoven, M. Blaauw, W. Pieters, and M. Warnier, "Privacy and information technology," in *The Stanford Encyclopedia of Philosophy*, Spring 2016 ed., E. N. Zalta, Ed., 2016.
- [3] A. F. Westin, *Privacy and freedom*, 1st ed. New York, NY, USA: Atheneum, 1967.
- [4] A. R. Miller, "Personal privacy in the computer age: The challenge of a new technology in an information-oriented society," *Michigan Law Review*, vol. 67, no. 6, pp. 1089–1246, 1969.
- [5] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. G. van Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the cost of cybercrime," in *The Economics of Information Security and Privacy*, R. Böhme, Ed. Berlin, Heidelberg, Germany: Springer, 2013, ch. 12, pp. 265–300.
- [6] R. van der Meulen and V. Woods, "Gartner survey shows more than 75 percent of companies are investing or planning to invest in big data in the next two years," Tech. Rep., 2015.
- [7] R. A. Rouse, "Is someone watching you through your webcam?" Tech. Rep., 2012.
- [8] F. Stutzman and J. Kramer-Duffield, "Friends only: Examining a privacy-enhancing behavior in facebook," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, New York, NY, USA, 2010, pp. 1553–1562.
- [9] J. F. George, "The theory of planned behavior and internet purchasing," *Internet research*, vol. 14, no. 3, pp. 198–212, 2004.
- [10] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," *Information Systems Research*, vol. 17, no. 1, pp. 61–80, 2006.
- [11] I. Ajzen, C. Timko, and J. B. White, "Self-monitoring and the attitude-behavior relation," *Journal of Personality and Social Psychology*, vol. 42, no. 3, pp. 426–435, 1982.
- [12] S. Spiekermann, J. Grossklags, and B. Berendt, "E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior," in *Proceedings of the 3rd ACM conference on Electronic Commerce (EC)*, New York, NY, USA, 2001, pp. 38–47.
- [13] B. Berendt, O. Günther, and S. Spiekermann, "Privacy in e-commerce: Stated preferences vs. actual behavior," *Communications of the ACM*, vol. 48, no. 4, pp. 101–106, 2005.
- [14] A. R. Beresford, D. Kübler, and S. Preibusch, "Unwillingness to pay for privacy: A field experiment," *Economics Letters*, vol. 117, no. 1, pp. 25–27, 2012.
- [15] F. J. Roethlisberger and W. J. Dickson, *Management and the worker: An account of a research program conducted by the Western electric Company, Hawthorne Works, Chicago*, 14th ed. Cambridge, MA, USA: Harvard University Press, 1939.
- [16] T. Hughes-Roberts, "Privacy and social networks: Is concern a valid indicator of intention and behaviour?" in *2013 International Conference on Social Computing (SocialCom)*, Washington, DC, USA, 2013, pp. 909–912.
- [17] K. Lewis, J. Kaufman, and N. Christakis, "The taste for privacy: An analysis of college student privacy settings in an online social network," *Journal of Computer-Mediated Communication*, vol. 14, no. 1, pp. 79–100, 2008.
- [18] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in *Proceedings of the 2005 ACM workshop on Privacy in the electronic society (WPES)*, Alexandria, VA, USA, 2005, pp. 71–80.
- [19] Kaspersky Lab; B2B International, "Actions to protect devices and online usage privacy according to internet users worldwide as of June 2015," Tech. Rep., 2015.
- [20] P. A. Norberg, D. R. Horne, and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of Consumer Affairs*, vol. 41, no. 1, pp. 100–126, 2007.
- [21] Z. Tufekci, "Can you see me now? Audience and disclosure regulation in online social network sites," *Bulletin of Science, Technology & Society*, vol. 28, no. 1, pp. 20–36, 2008.
- [22] S. B. Barnes, "A privacy paradox: Social networking in the United States," *First Monday*, vol. 11, no. 9, 2006.
- [23] M. Taddicken, "The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure," *Journal of Computer-Mediated Communication*, vol. 19, no. 2, pp. 248–273, 2014.
- [24] B. Reynolds, J. Venkatanathan, J. Gonçalves, and V. Kostakos, "Sharing ephemeral information in online social networks: Privacy perceptions and behaviours," in *Human-Computer Interaction (INTERACT)*, Lisbon, Portugal, 2011, pp. 204–215.
- [25] S. Utz and N. Krämer, "The privacy paradox on social network sites revisited: The role of individual characteristics and group norms," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, vol. 3, no. 2, pp. 1–10, 2009.

- [26] G. Blank, G. Bolsover, and E. Dubois, "A new privacy paradox: Young people and privacy on social network sites," in *Annual meeting of the American Sociological Association (ACA)*, vol. 17, San Francisco, CA, USA, 2014.
- [27] A. L. Young and A. Quan-Haase, "Privacy protection strategies on facebook: The internet privacy paradox revisited," *Information, Communication & Society*, vol. 16, no. 4, pp. 479–500, 2013.
- [28] E. Christofides, A. Muise, and S. Desmarais, "Information disclosure and control on facebook: Are they two sides of the same coin or two different processes?" *Cyberpsychology & Behavior: The impact of the internet, multimedia and virtual reality on behavior and society*, vol. 12, no. 3, pp. 341–345, 2009.
- [29] C. Lutz and P. Strathoff, "Privacy concerns and online behavior – not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses," in *Multinationale Unternehmen und Institutionen im Wandel - Herausforderungen für Wirtschaft, Recht und Gesellschaft*, 1st ed. Bern, Switzerland: Stämpfli Verlag, 2013, ch. 8, pp. 81–99.
- [30] T. Dienlin and S. Trepte, "Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors," *European Journal of Social Psychology*, vol. 45, no. 3, pp. 285–297, 2015.
- [31] I. Ajzen, "The theory of planned behavior," *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 179–211, 1991.
- [32] —, *Attitudes, personality, and behavior*. Homewood, IL, US: Open University Press, 1988.
- [33] S. Sutton, "Predicting and explaining intentions and behavior: How well are we doing?" *Journal of Applied Social Psychology*, vol. 28, no. 15, pp. 1317–1338, 1998.
- [34] M. Fishbein and I. Ajzen, *Belief, attitude, intention and behavior: An introduction to theory and research*. Reading, MA, USA: Addison-Wesley, 1975.
- [35] I. Ajzen and M. Fishbein, *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ, USA: Prentice Hall, 1980.
- [36] D. M. Randall and J. A. Wolff, "The time interval in the intention-behaviour relationship: Meta-analysis," *British Journal of Social Psychology*, vol. 33, no. 4, pp. 405–418, 1994.
- [37] S. Engelhardt and A. Narayanan, "Online tracking: A 1-million-site measurement and analysis," Tech. Rep., 2016.
- [38] R. S. Portnoff, L. N. Lee, S. Egelman, P. Mishra, D. Leung, and D. Wagner, "Somebody's watching me?: Assessing the effectiveness of webcam indicator lights," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI)*, Seoul, Republic of Korea, 2015, pp. 1649–1658.
- [39] R Core Team, "R: A language and environment for statistical computing," Vienna, Austria, Tech. Rep., 2013. [Online]. Available: <http://www.R-project.org/>
- [40] D. P. MacKinnon, J. L. Krull, and C. M. Lockwood, "Equivalence of the mediation, confounding and suppression effect," *Prevention Science*, vol. 1, no. 4, pp. 173–181, 2000.

## Appendix

Table 5. Original Question Wording

Item code	Item
<i>Attitudes towards webcam covers</i>	
AW1	Ich habe Angst, dass jemand unautorisiert auf meine Webcam zugreifen kann
AW2	Ich bin der Meinung, man sollte sich vor unautorisiertem Zugriff auf die eigene Webcam schützen
AW3	Ich erachte das Abdecken der Webcam als eine übertriebene Vorsichtsmaßnahme
AW4	Ich halte Webcam-Abdeckungen für praktisch
AW5	Ich halte Webcam-Abdeckungen für nützlich
AW6	Ich halte Webcam-Abdeckungen für notwendig
AW7	Ich halte Webcam-Abdeckungen für sicher
<i>Attitudes towards privacy</i>	
AP1	Ich bin der Meinung, Videokameras sollten an öffentlichen Orten eingesetzt werden, um die allgemeine Sicherheit zu steigern
AP2	Ich halte es für unbedenklich, persönliche Informationen über mich auf sozialen Netzwerken (wie z. B. <i>facebook</i> ) preis zu geben
AP3	Ich würde ein Video von mir auf einer öffentlich zugänglichen Webseite hochladen
AP4	Ich glaube, dass der Staat meine Privatsphäre im Internet ausreichend schützt
AP5	Ich glaube, dass Unternehmen meine Privatsphäre respektieren
<i>Subjective norms towards webcam covers</i>	
SW1	Viele Leute in meinem Umfeld decken ihre Webcam ab
SW2	Viele Leute in meinem Umfeld sind der Meinung, ich sollte meine Webcam abdecken
SW3	Es wird in meinem Arbeitsumfeld von mir erwartet, dass ich meine Webcam abdecke
SW4	Ich befürchte, dass meine Umwelt mich für übertrieben vorsichtig hält, wenn ich meine Webcam abklebe
<i>Subjective norms towards privacy</i>	
SP1	Ich denke, es wird gesellschaftlich von mir erwartet, meine Privatsphäre selbst im Internet zu schützen
SP2	In meinem Umfeld ist der Schutz der Privatsphäre ein wichtiges Thema
SP3	Ich befürchte Ablehnung seitens meines Umfelds, wenn ich nicht in sozialen Netzwerken (wie z. B. <i>facebook</i> ) aktiv bin
SP4	Ich befürchte Ablehnung seitens meines Umfelds, wenn ich keine Bilder von mir in sozialen Netzwerken (wie z. B. <i>facebook</i> ) teile
<i>Additional open questions</i>	
AQ1	Falls Sie Ihre Webcam momentan abgedeckt haben, wie lange ist dies bereits der Fall?
AQ2	Falls Sie Ihre Webcam am Laptop momentan nicht abgedeckt haben, haben Sie dies in der Vergangenheit getan? Wenn ja, wieso ist dies nicht mehr der Fall?



Table 6. Descriptive Statistics for All Items

Item code	Item description	Total ( $n = 100$ )		With cover ( $n = 32$ )		Without cover ( $n = 78$ )	
		Mean	SD	Mean	SD	Mean	SD
<i>Attitudes towards webcam covers</i>							
AW1	Fear of unauthorized webcam access	4.09	1.75	4.59	1.72	3.85	1.73
AW2	Opinion that one should protect from unauthorized webcam access	5.13	1.58	5.53	1.59	4.94	1.55
AW3	Perception that webcam covering is excessively cautious	3.42	1.76	2.34	1.68	3.93	1.58
AW4	<b>Perception that webcam covers are practical</b>	<b>4.27</b>	<b>1.98</b>	<b>5.56</b>	<b>1.48</b>	<b>3.67</b>	<b>1.90</b>
AW5	Perception that webcam covers are useful	5.33	1.65	6.38	0.75	4.84	1.73
AW6	<b>Perception that webcam covers are necessary</b>	<b>4.55</b>	<b>1.90</b>	<b>6.16</b>	<b>1.25</b>	<b>3.79</b>	<b>1.67</b>
AW7	Perception that webcam covers are secure	5.61	1.47	6.06	1.13	5.40	1.57
<i>Attitudes towards privacy</i>							
AP1	Opinion that video cameras should be used at public places to increase security	4.06	1.76	3.78	1.64	4.19	1.81
AP2	Perception that the disclosure of own personal information in social networks is harmless	2.46	1.42	1.97	0.82	2.69	1.58
AP3	Willingness to upload a personal video on a public website	2.58	1.60	2.16	1.32	2.78	1.68
AP4	<b>Belief that the government sufficiently protects personal privacy on the Internet</b>	<b>2.31</b>	<b>1.18</b>	<b>2.12</b>	<b>1.13</b>	<b>2.40</b>	<b>1.20</b>
AP5	<b>Belief that firms respect personal privacy</b>	<b>2.36</b>	<b>1.40</b>	<b>2.31</b>	<b>1.38</b>	<b>2.38</b>	<b>1.43</b>
<i>Subjective norms towards webcam covers</i>							
SW1	<b>People in the social environment use a webcam cover</b>	<b>4.70</b>	<b>1.71</b>	<b>5.03</b>	<b>1.53</b>	<b>4.54</b>	<b>1.77</b>
SW2	<b>People in the social environment argue for webcam covering</b>	<b>3.57</b>	<b>1.70</b>	<b>4.42</b>	<b>1.60</b>	<b>3.18</b>	<b>1.61</b>
SW3	Expectation of others to use a webcam cover in the work environment	1.92	1.29	2.59	1.34	1.60	1.15
SW4	Fear that others rate webcam covering overly cautious	2.62	1.37	2.53	1.24	2.66	1.43
<i>Subjective norms towards privacy</i>							
SP1	Perception that society expects Internet privacy self-protection	4.55	1.53	4.44	1.54	4.60	1.53
SP2	Privacy protection is an important topic in the social environment	4.36	1.45	4.75	1.55	4.18	1.38
SP3	Fear of social rejection for not being active in social networks	2.77	1.64	2.78	1.77	2.76	1.58
SP4	Fear of social rejection for not sharing pictures in social networks	1.84	1.14	1.78	1.10	1.87	1.17

SD = standard deviation

Items that turned out to have a significant impact on behavior are depicted in **bold**