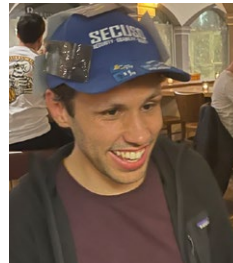


Liebe Leserinnen und Leser,

2022 war ein ereignisreiches Jahr: Von strengen Corona-Regeln, zu vielen Lockerungen aber gleichzeitig neuen Problemen durch den Ukraine-Krieg. Wir als SECUSO haben dennoch versucht das Beste aus der Situation und der mobilen Arbeit zu machen und weiter daran geforscht, wie wir Sicherheitsmaßnahmen für Bürger und Bürgerinnen benutzbarer gestalten können. Neben spannenden Forschungsergebnissen (mehr dazu auf den Flyer-Innenseiten) hat sich auch im Team bzw. bei den Alumni einiges getan:

- Peter Mayer hat eine Juniorprofessur an die University South Denmark angenommen, unterstützt uns zum Glück weiterhin in Nebentätigkeit
- Oksana Kulyk ist an der IT University Copenhagen zur Associate Professorin befördert worden
- Jurlind Budurushi hat eine Stelle als Lecturer an der Qatar University angenommen.
- Neu im Team sind: Fabian Ballreich, Tobias Hilt, Tobias Länge, Philipp Matheis, Dirk Müllmann, sowie die Studentischen Hilfskräfte: Elena, Leoni, Miria und Patrick



Herzlich bedanken möchten wir uns bei Christopher Beckmann, der nun seinem Traumberuf als Pen-Tester nachgeht, und Heike Dietmann, die wieder als Lehrerin arbeitet, für die gute (und immer noch andauernde) Zusammenarbeit.

Wir freuen uns, dass wir dieses Jahr gleich zwei Preise für unsere Arbeit erhalten

haben und für zwei weitere Preise nominiert wurden. Erhalten haben wir den Digital Autonomy Award (von GI/BMBF) und den Deutschen Verbraucherschutzpreis (Deutsche Stiftung Verbraucherschutz/BMU). Nominiert wurden wir u.a. für den Deutschen IT-Sicherheitspreis mit SMILE-4-VIP: Einem Ansatz, der insbesondere Blinde dabei unterstützt, Phishing E-Mails einfacher zu erkennen. Wir freuen uns an



diesem Projekt gemeinsam mit dem Zentrum für digitale Barrierefreiheit und Assistive Technologien (ACCESS) in 2023 weiter zu arbeiten.

Der Fokus im Bereich der Security Awareness lag 2022 auf neuen Umsetzungsformen. So begleitete uns z.B. das neue

Team-Mitglied P. STAR, der Security Teaching & Awareness Robot, zur Hannover Messe und zur Nacht der Wissenschaften konnte ein Touchable mit Phishing- und Passwort-Spiel in der Triangel ausprobiert werden. Der Phishing-Master wurde weiterentwickelt und stand Besuchern des ZKM zum Spielen zur Verfügung. Das NoPhish Quiz steht nun auch über die Plattform wir-forschen-digital.de zur Verfügung. Nicht zu vergessen ist unser NoPhish Video III, welches gemeinsam mit der Agentur motionensemble erstellt wurde. Für 2023 steht der Abschluss der Evaluation eines NoPhish-Karten-Spiels und eines Challenge-Parcours für SchülerInnen an. Unser Angebot für BürgerInnen wächst also jedes Jahr. Es sollte für jeden etwas dabei sein, um sich effektiv gegen Phishing zu schützen.



Trotz der erschwerten Bedingungen, fanden einige Group Activities des SECUSO Teams, wie Wanderungen durch Karlsruhe, ein Kicker-Turnier, ein Mini-Golf-Turnier im Dunkeln und diverse Abendessen statt. Auch der Karlsruher Monthly Security&Privacy Lunch ist im Sommer wieder gestartet und findet in Kooperation mit der 2022 neu gegründeten KIT Graduate School Cyber Security statt. Zuletzt hatten wir durch die Lockerungen die Möglichkeit erste Gäste der Distinguished Lecture Series in Cyber Security vor Ort zu begrüßen - genau wie Gäste des SECUSO Research Seminars. Zuletzt sei erwähnt, dass wir seit diesem Jahr auch auf Mastodon unterwegs sind - mit bereits über 650 Folgenden.



Das Team von SECUSO wünscht frohe Weihnachten, schöne Feiertage und einen guten Rutsch ins neue Jahr!

Wir bedanken uns für die Zusammenarbeit in der Vergangenheit und freuen uns auf Kooperationen in 2022!

Maxime Veit

Lukas Aldag

MATTIA MOSSANO

Fabian Ballreich

Melanie Volkmann

Rebecca Golling

Peter Mayer

Henri Schmidt-Eck

Miriam Kutter

Mark Bohlender

Tobias Länge

Benjamin Bernig

Dirk Müllmann

Anne Hennig

Patrick Schneider

Philipp Matheis



Weihnachtspost von SECUSO

Rückblick auf das Jahr 2022

INSTITUT FÜR ANGEWANDTE INFORMATIK UND FORMALE BESCHREIBUNGSVERFAHREN (AIFB)



SECUSO
SECURITY · USABILITY · SOCIETY



Veröffentlichungen

E-MAIL SICHERHEIT (6)

- Development and Evaluation of an Anti-Phishing Shooting Game, *open access*
- Poster: The Phishing Master Anti-Phishing Game, *ACSAC*
- Design and Evaluation of an Anti-Phishing Artifact Based on Useful Transparency, *STAST@ESORICS*
- Phishing awareness and education – When to best remind?, *USEC@NDSS*
- „I don't know why I check this..." - Investigating Expert Users' Strategies to Detect Email Signature Spoofing Attacks, *SOUPS*
- Technische & Rechtliche Auseinandersetzung mit Weiterleitungs-URLs in E-Mails aus Security Gründen, *Recht&Informatik@Informatik*

ONLINE-WAHLEN (6)

- Council of Europe Guidelines on the Use of ICT in Electoral Processes, *EIS@ESORICS*
- Increasing security without decreasing usability: A comparison of various verifiable voting systems, *SOUPS*
- Why is Online Voting Still Largely a Black Box, *EIS@ESORICS*
- German voters' attitudes towards voting online with a verifiable system, *VOTING@FC*
- Recent Developments in the Context of Online Elections and Digital Polls in Germany, *Sicherheit*
- Research Opportunities in Evidence-Based Elections, *CRA*

AUTHENTIFIZIERUNG (5)

- Why Users (Don't) Use Password Managers at a Large Educational Institutions, *USENIX Security*
- Poster: PassSec+ - An add-on that protects your passwords, payment data and privacy, *SOUPS*
- SoK: A Systematic Literature Review of Knowledge-Based Authentication on Augmented Reality Head-Mounted Displays, *ARES*
- Shoulder-Surfing Resistant Authentication for Augmented Reality, *NordiCHI*
- PassGlobe: Ein Shoulder-Surfing resistentes Authentifizierungsverfahren für Virtual Reality Head-Mounted Displays, *Workshop@MUC*

COOKIES (3)

- Cookie Disclaimers: Impact of Design and Users' Attitude, *ARES*
- Your Cookie Disclaimer is not in line with the ideas of the GDPR. Why?, *HAISA*
- Manipulative Designs von Cookies – *DuD*

NOTIFICATION MESSAGES (2)

- Poster: Standing out among the daily spam: How to catch website owners' attention by means of vulnerability notifications, *CHI*
- Your website has been hijacked: Raising awareness for an invisible problem, *PhD@Sicherheit*

Projekte

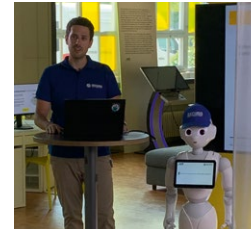
- KD²Ex (KIT-Exzellenzuniversität), Authentifizierung mit AR/VR (Facebook/Meta), Effektive Security Awareness am KIT, Vertrauen durch Erklärbarkeit bei verifizierbaren Online-Wahl-Systemen (KIT Bereichsprojekt), Ende-zu-Ende-verifizierbare und geheime Online-Wahlen am KIT (KIT-Strategiefond)
- ESS (Helmholtz-Gemeinschaft) – Koordination der Forschungsgruppe Human&Societal Factors
- Digilog (Land BW); INSPECTION (BMBF)
- Phishing Warnings (Google), Authentifizierung mit AR/VR (Facebook/Meta)

Gäste

- *Visiting Researchers as KIT International Fellow*: Prof. Dr. K. Renaud (Strathclyde University)
- *KASTEL Distinguished Lecture Series*: Prof. Dr. A. Sasse (Ruhr-Uni Bochum), Prof. Dr. L. o Cavallaro (University College London), Prof. Dr. O. Lynskey (London School of Economics)
- *Research seminar guests*: D. Ruescas (Sequent), Dr. B. Stock (CISPA), Prof. Dr. S. Trang (Uni Göttingen), Dr. D. Dueñas-Cid (Gdansk University of Technology), Prof. Dr. C. Krauß (hda), M. Krüger (DEMOCRACY - Deutschland), B. Bachman (Ströer SE & Co. KGaA), Prof. Dr. O. Kulyk (IT University of Copenhagen), Prof. Dr. V. Teague (Australian National University), S. Roth (CISPA), Prof. Dr. N. Ebert (ZHAW), A. Harbrecht (aramido GmbH), Prof. Dr. C. Reuter (TU Da), Prof. Dr. J. Benaloh (Microsoft Research / University of Washington), L. Struppek (TU Da), M. Bahrini (Uni Bremen), M. Brinkmann (Ruhr-Uni Bochum)

Vorträge (außerhalb von wissenschaftl. Konferenzen/Workshops), Panels und Interviews (Auswahl)

- Vortrag im Rahmen des Fachgespräch im Bundestag zu E-Voting
- Vortrag beim Swiss Website Security Day zu „Your website has been hacked – ...“
- Vortrag beim BigTechday zu „Usable Security @KIT“
- Vortrag zum Security Day zu „Security Awareness - ganz oder gar nicht?“
- Vortrag zu „Digital Self Defense against Phishing“ bei Ostessen Metall



- Vorstellung des Projekts Inspection bei den IT-Sicherheitsbeauftragten der IHK
- Vortrag bei der Deutschen Flugsicherung zu „Security and Privacy for everyone“
- Vortrag zum Mobile World Congress zu „Secure your success - it's a CXO topic“
- Vortrag im BSI-Format DVS Open zu „...Fake Shops erkennen und behandeln“
- Paneldiskussion@Sicherheit 2022 „Warum ... Blackbox-Online-Wahlssystemen ...?“
- Paneldiskussion@Deutscher IT-Sicherheitskongress „Cyber-Sicherheit ist Chefinnen- und Chefsache!“
- Interview „Phishing-Training - Von Sinn und Unsinn der Tests und Simulationen“ im Security Awareness Insider Podcast
- Interview „IT Security kann nur funktionieren, wenn alle mitmachen - doch wie schafft man Awareness bei den Mitarbeiter*innen?“ im Espresso Talk
- Interview „Die verflixte PIN“ im WDR
- Interview „Bei uns wird es nie Tracking oder Werbung geben“ in Golem.de
- Interview „Vergesst vergessene oder unsichere Passwörter“ im SWR

Mitgliedschaften

- PC Member (Auswahl): SOUPS, EuroUSEC, ACSAC, SPOSE, EIS, ARES, E-Vote ID
- Mitgliedschaften: Editorial Board: ACM ToPS, Acedemy Member ARRTI@KIT

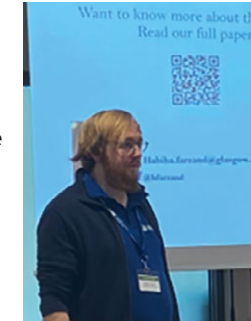
Abschlussarbeiten

8 Abschlussarbeiten wurden fertiggestellt von denen 4 von Masterstudenten bearbeitet wurden, die auch das KASTEL Zertifikat erhalten haben:

- Entwicklung und Evaluation von Schulungsmaterial zur Verwendung von S/MIME (Master)
- Entwicklung von Shoulder-Surfing resistenten Authentifizierungsmethoden für VR HMDs (2 Master)
- Development of Shoulder-Surfing Resistant Authentication Schemes for Augmented Reality Head-Mounted Displays (Master)
- Effektive Phishing-Sensibilisierung bei unterschiedlichen Vorkenntnissen: Eine Studie zur Evaluation des NoPhish Cardgames (Bachelor)
- A usability study of a TORPEDO expansion for mobile devices (Bachelor)
- Untersuchung der Effektivität von Return Code basierten (Bachelor)
- „Ihre Website wurde gehackt“ - Wie wurden Website-Besitzer:innen über Sicherheitslücken auf ihren Websites informiert? (Bachelor)

Lehre

Bachelor-Vorlesung Informationssicherheit, Master-Vorlesung Human Factors in Security



SEMINAR

E-Voting (mit den Forschungsgruppen ‚Anwendungsorientierte Formale Verifikation‘ und ‚Kryptographie und Sicherheit‘), *Internet und Gesellschaft* (mit der Forschungsgruppe Dezentrale Systeme und Netzdienste, dem Institut für Telematik Forschungsgruppe und dem Institut für Informations- und Wirtschaftsrecht, *Informationssicherheit und Datenschutz* (mit der Forschungsgruppe ‚Betriebliche Informationssysteme‘), *Digital Citizen Science* (mit den Forschungsgruppen ‚Information Systems & Service Design‘, ‚Human Resource Management‘, ‚Cognition and Consumer Behavior‘, ‚Politische Ökonomie‘ und ‚Information & Market Engineering‘ und dem Institut für Sport und Sportwissenschaft), *Security und Privacy Awareness* (mit dem Institut für Philosophie und dem Zentrum für Angewandte Rechtswissenschaft)

PRAKTIKA

Security, Usability and Society (mit der Forschungsgruppe ‚Praktische IT-Sicherheit‘), KASTEL Praktikum (mit den Forschungsgruppen ‚Kryptographie und Sicherheit‘ und ‚Effiziente Algorithmen‘ sowie dem Institut für Telematik und dem FZI), Teamprojekt Softwareentwicklung (mit dem Institut für Telematik, dem Institut für Informationssicherheit und Verlässlichkeit, dem Institut für Wirtschaftsinformatik und Marketing & dem Institut für Angewandte Betriebswirtschaftslehre und Unternehmensführung)

Events (Teilnahme & Organisation)

Mit STAR und dem Phishing Master auf der *Hannover Messe*, mit Phishing- und Passwort Quiz auf dem Touchtable bei der *Langen Nacht der Wissenschaft*, Phishing Experiment zur *Bunten Nacht der Digitalisierung*, Präsentation STAR zum „*Today I Learned*“ (TIL) Festival im Triangel Open Space, Cybersecurity Workshop als *Benefizveranstaltung für die Ukraine*, Workshop „*Digital Self Defense*“ zum *bundesweiten Digitaltag*, Local Organizer *EuroUSEC 2022*

