Karlsruher Institut für Technologie

KASTEL-Praktikum Sicherheit

PD Dr.-Ing. Ingmar Baumgart <baumgart@fzi.de>

KOMPETENZZENTRUM FÜR ANGEWANDTE SICHERHEITSTECHNOLOGIE (KASTEL)

KASTEL-Praktikum Sicherheit

Ziele

- IT-Sicherheit im Alltag bewerten
- Erkennen, wo/wie Sicherheitsmechanismen nicht wirken
- Lernen, wie Sicherheit korrekt umgesetzt wird

Zielgruppe

- Studierende mit Spaß am „hacken“ = Dinge anders als vorgesehen nutzen

Organisatorisch

- Interdisziplinäres Praktikum, Teil von KASTEL
  - Mehrere Lehrstühle am KIT
  - Fraunhofer IOSB
  - FZI Forschungszentrum Informatik
  - LKA Landeskriminalamt Baden-Württemberg
- Vortrag als Blockveranstaltung Ende Januar / Anfang Februar

Format

- Praktikumsgruppen à 2 Studenten
- Selbstständige Arbeit wird erwartet
- Regelmäßige Treffen mit Betreuer zur Abstimmung
- Vorträge und Demos während des Semester, mit Anwesenheitspflicht!
- Anrechenbar für das KASTEL-Zertifikat

- Erwartete Ergebnisse
  - Abschlussvortrag mit Demonstration(en), 45 - 60 Minuten
  - Ausarbeitung / Dokumentation, 10 – 15 Seiten
    - Abgabe spätestens **2 Wochen** nach der Präsentation

Fakultät Informatik

- Praktikum, 4 ECTS

Fakultät Wirtschaftswissenschaften

- Praktikum, 4 ECTS

vorläufig

DIE THEMEN WS 2018/19

Efail

Betreuer: FZI (Müller) / FZI (Hackenjos)

- Schwachstellen in vielen verbreiteten E-Mail-Programmen
  - Exfiltration von verschlüsselten Nachrichten (PGP und S/MIME)
  - Fehlende Integritätsprüfung von Chiffraten
  - Unterschiedliche Rückkanäle möglich (HTTP, OCSP, CRL, …)
  - Patches für PGP
  - S/MIME erfordert Änderungen an der Spezifikation
- Aufgabe:
  - Nachstellen der Schwachstellen
  - Vergleich unterschiedliche Rückkanäle
- Literatur
  - https://efail.de/efail-attack-paper.pdf

Social-Engineering-Attack using „Free Wifi“

Supervisor:

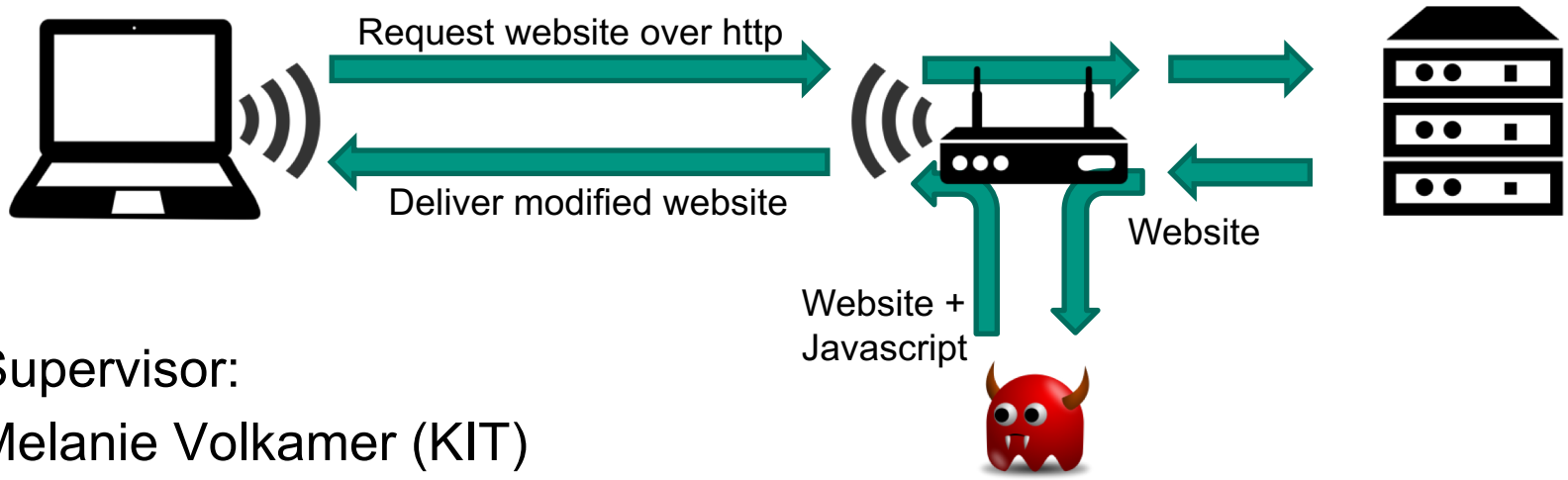
Peter Mayer (KIT)

Task

- Highlevel: Be the „good bad guy“
  - Social Engineering attack with „free wifi“ in multiple locations around town
  - Intercept traffic in this wifi
  - Warn users when they submit data unencrypted (no ssl, no vpn, etc.)
- In detail
  - Adapt „openwrt-traffic-analyzer“ & „openwrt-homographic-wifi-cloner“
  - Analysis of unencrypted traffic
  - Analyse which types of traffic are sent unencrypted
  - Test which wifi-names work best
  - Create suitable captive portal and landing pages

Laptop by Theresa Berens from the Noun Project. Router by Guilherme Furtado from the Noun Project. Server by Mister Pixel from the Noun Project.

Attack on unencrypted traffic



Supervisor:

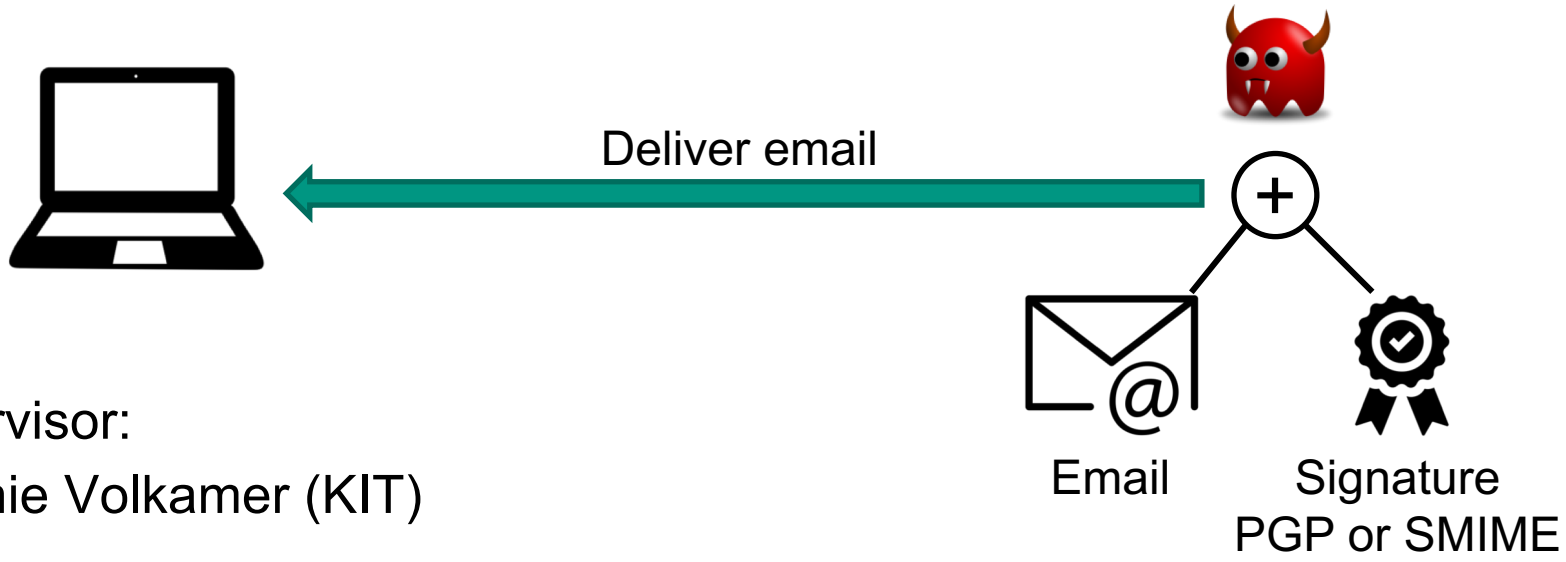
Melanie Volkamer (KIT)

Task

- Highlevel:
  - Inject additional javascript into unencrypted websites
- In detail:
  - Create Access Point configured to perform injection-attack
  - Create payloads with different functionality

Laptop by Theresa Berens from the Noun Project. Router by Guilherme Furtado from the Noun Project. Server by Mister Pixel from the Noun Project.

Signature Spoofing



Supervisor:
Melanie Volkamer (KIT)

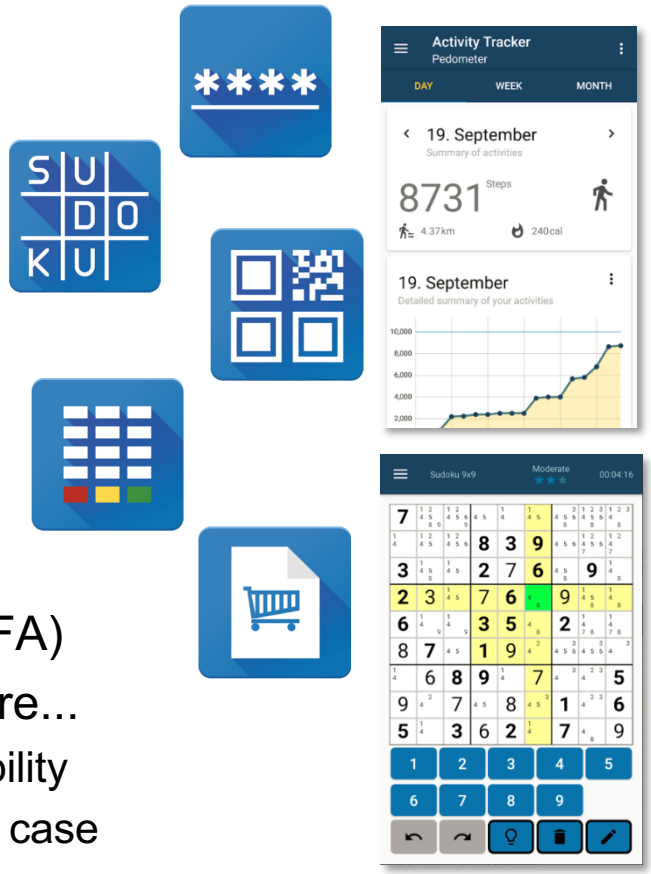
Task

- Highlevel:
  - Advanced Social Engineering attack using spoofed signatures on emails
- In detail:
  - Tool to compose emails (html formatting for easy cloning of existing mails)
  - Allow creation of signatures using arbitrary PGP and S/MIME keys

Laptop by Theresa Berens from the Noun Project. Email by Creative Stall from the Noun Project. Certificate by Gregor Cresnar from the Noun Project.

Development of Privacy Friendly Apps

Privacy Friendly Apps



Supervisor:

Christopher Beckmann (KIT)

Task

- Highlevel:
  - Development of a Privacy Friendly App (PFA)
  - PFAs are open source android apps that are...
    - ...optimised with regard to privacy and usability
    - ...use minimal permissions to fulfil their use case
- In detail:
  - Topics vary each semester and are usually done in teams of two students
  - Past topics include: WeatherApp, Sudoku, ToDo-List, CircuitTrainer, etc.

Webseite

https://ilias.studium.kit.edu/goto.php?target=crs_719271&client_id=produktiv

- „KASTEL-Praktikum Sicherheit“ in WS 2018/2019
- Passwort für die Kursregistrierung: