SEMINAR: NEXT GENERATION SECURE COMPUTER ARCHITECTURES – INTRODUCTION

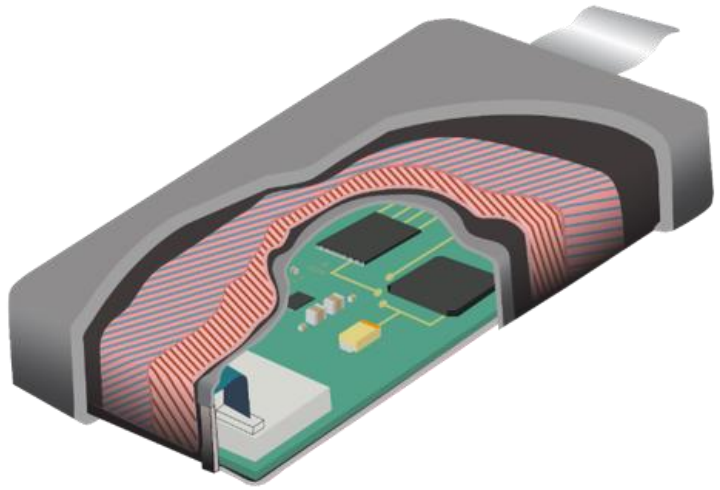
Matthias Hiller, Lukas Auer, Vincent Immler

Physical Security Technologies Group

TUM Contact: Thomas Kittel, Chair for IT Security

Physical Security Technologies Group @ Fraunhofer AISEC

- Tamper Protection for Embedded Systems
  - Tamper Sensor Design
  - Circuits / Algorithms
  - **Architectures** for Embedded Systems
  - Secure Boot / RTOS
- System on Chip Design
  - **Security Architecture**
- And other Lower-Level Topics close to Electrical Engineering and Technical Informatics …



Prerequisites for this Seminar

- BSc / MSc student of Informatics
- Background in Computer Architecture
- Interest in IT Security

Schedule

DATE	TIME	LOCATION	
06.02.18	09:30	01.08.033	Introduction
09.-14.02.18			Registration
27.04.18	10:00-12:00	01.08.033	Paper Writing / Presentation Training
14.06.18	23:59		Submission Deadline Papers
25.06.18	23:59		Submission Deadline Presentations
28.06.18	09:00-18:00	01.08.033	Final Presentations
29.06.18	09:00-18:00	01.08.033	Final Presentations

27.04.18 Training on Scientific Writing and Presentation

- How to write a good paper
  - Technical writing
  - Level of abstraction
  - Storyline
  - Language and style
- How to give a good presentation
  - Know your audience
  - What do you want to communicate?
  - Trade-off between technical precision and capturing the audience

Writing

- Extract the main points, explain and simplify theory, give a survey over related work

- LNCS Template provided via moodle
- 10-12 Pages Content, References not included
- Written in English

Presentation

- Scientific Presentation
- Conference Style
- 25 mins Presentation + 5 min Q/A

Grading

- Presence in presentation/writing training and final discussions is mandatory (if you have a good reason that you cannot attend, please let me know)
- Final Grade:
  - 50% Writing
  - 50% Presentation
- Drop-out after Matching -> Grade 5.0

Topics and Advisors (firstname.lastname@aisec.fraunhofer.de)

- AEGIS: Architecture for Tamper-Evident and Tamper-Resistant Processing (Matthias Hiller)
- Oblivious RAM Protocols (Matthias Hiller)
- Invasive Computing (Vincent Immler)
- Formal Foundation for Secure Remote Execution of Enclave (Vincent Immler)

* Other topics are possible on request before registration

- Survey over Intel SGX Extensions and ARM TrustZone (Lukas Auer)
- Sanctum Hardware Extensions for Strong Software Isolation (Lukas Auer)
- The CHERI capability model: Revisiting RISC in an age of risk (Lukas Auer)
- CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds (Lukas Auer)

Registration

Please register through the matching system

http://docmatching.in.tum.de

Contact Information

Dr.-Ing. Matthias Hiller
Head of Physical Security Technologies Group

Fraunhofer Institute for
Applied and Integrated Security AISEC

Parkring 4
85748 Garching (near Munich)
Germany

www.aisec.fraunhofer.de

Phone +49 (0)89 3229986-162
matthias.hiller@aisec.fraunhofer.de