Next Generation Secure Computer Architectures

Seminare 2 SWS / 5 ECTS (Kursbeschreibung)
Veranstalter: Thomas Kittel
Beginn:

Vorbesprechung: Di, 06.2. um 09:30 Uhr im Raum 01.08.033 [Folien]

Termine (geplant):

- Zwischenevaluation:
  - Fr, 27.04.2018 - 10-12 Uhr - 01.08.033
- Vorträge:
  - Do, 28.06.2018 - 09-18 Uhr - 01.08.033
  - Fr, 29.06.2018 - 09-18 Uhr - 01.08.033

Verantwortliche:

- Matthias Hiller
- Lukas Auer
- Vincent Immler

Mögliche Themen umfassen:

- AEGIS: Architecture for Tamper-Evident and Tamper-Resistant Processing
  - AEGIS is a processor architecture, secure against both physical and software attacks. It assumes that all external components, as well as the operation system, are untrustable. Physical and software tampering is detected by tamper-evident and authenticated environments. In addition, environments are private to prevent an adversary from obtaining information by tampering with or observing system operation.
    - https://www.princeton.edu/~rblee/ELE572Papers/Fall04Readings/AEGIS_Suh.pdf
    - http://csg.csail.mit.edu/pubs/memos/Memo-461/memo-461.pdf

- Oblivious RAM Protocols
  - Oblivious RAM (ORAM) prevents access pattern leakage to hide the sequence of operations being performed. Specifically, the sequence in which memory locations are accessed is equivalent for all inputs with the same access time. ORAM solutions provide strong privacy guarantees since an observer is unable to distinguish accesses from random. They are used in applications such as secure cloud storage, secure multi-party computation, and secure processors.
    - https://acmccs.github.io/papers/p523-doernerA.pdf
    - https://acmccs.github.io/papers/p507-rocheA.pdf
    - http://web.cs.ucla.edu/~rafail/PUBLIC/09.pdf

- Survey over Intel SGX Extensions and ARM TrustZone
  - Intel Software Guard Extensions (SGX) allows user-code to run in isolated memory regions (enclaves), which are protected from code running at higher privilege levels. It aims to provide integrity and confidentiality guarantees (secure remote computation) in a potentially malicious software environment.
    - https://eprint.iacr.org/2016/086.pdf

- Sanctum Hardware Extensions for Strong Software Isolation
  - Sanctum is an alternative to Intel's Software Guard Extensions (SGX). It provides strong provable isolation of software modules running concurrently with shared resources. Unlike SGX, which is implemented in microcode, Sanctum is mostly implemented with trusted software and is therefore easier to analyze. A prototype of the extension is implemented with the Rocket RISC-V core.
    - https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_costan.pdf
    - https://github.com/pwnall/sanctum

- The CHERI capability model: Revisiting RISC in an age of risk
  - CHERI (Capability Hardware Enhanced RISC Instructions) is an extension to 64-bit RISC instruction set architectures (ISA). It introduces a hybrid capability-system to allow software to efficiently implement fine-grained memory protection policies and software compartmentalization. FreeBSD and the LLVM compiler have been modified to take advantage of the CHERI extension.
    - https://www.cl.cam.ac.uk/research/security/ctsrd/pdfs/201406-isca2014-cheri.pdf
    - https://www.cl.cam.ac.uk/research/security/ctsrd/pdfs/201505-oakland2015-cheri-compartmentalization.pdf
    - https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-907.pdf
    - https://www.cl.cam.ac.uk/research/security/ctsrd/cheri/

- CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds
  - CHAINIAC is a decentralized software-update framework with the goal of eliminating single points of failure, enforcing transparency, and providing efficient verifiability of integrity and authenticity. Signed software-updates are collected in a tamper-proof release log based on the skipchain, a cryptographically-traversable, offline- and peer-to-peer-verifiable blockchain structure.
    - https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-nikitin.pdf
    - https://www.usenix.org/sites/default/files/conference/protected-files/usenixsecurity17_slides_nikitin.pdf
    - https://bford.github.io/2017/08/01/skipchain/

- Invasive Computing
  - Invasive computing is a new processing paradigm for Multi-Processor Systems-on-Chip (MPSoCs). Programs can dynamically scale from running on just one processor to multiple, neighboring processors. This first phase of expanding to multiple processors is the invasion step. After the highly parallel processing phase, programs scale the consumed resources back in the retreat step.
    - https://invasic.informatik.uni-erlangen.de/publications/invasic-overview.pdf

- Formal Foundation for Secure Remote Execution of Enclave
  - This paper introduces a verification methodology for trusted hardware platforms such as Intel SGX and the MIT Sanctum extension. It formalizes an idealized enclave platform along with a parameterized adversary. In addition, it formalizes the notion of secure remote execution and presents machine-checked proofs for its three key security properties: integrity, confidentiality, and secure measurement.
    - https://people.eecs.berkeley.edu/~rsinha/research/pubs/ccs2017.pdf

- Weitere Themenvorschläge durch Studierende können berücksichtigt werden.

Upcoming Events

- MA Abschlussvortrag Christopher Sendlinger / Kilian Tscharke, Pascal Debus
  Jan 16, 2025 10:00 AM
  (Europe/Berlin) — per Videokonferenz
- MA Abschlussvortrag Boris-Chengbiao Zhou / Fabian Franzen
  Jan 16, 2025 01:00 PM
  (Europe/Berlin) — per Videokonferenz
- MA Abschlussvortrag Jason Lochert / Sebastian Peters, David Emeis, Lukas Lautenschlager
  Jan 23, 2025 11:00 AM
  (Europe/Berlin) — per Videokonferenz
- BA Abschlussvortrag Leon Birkel / Fabian Franzen
  Jan 28, 2025 03:00 PM
  (Europe/Berlin) — per Videokonferenz

Previous events…
Upcoming events…

News

- Prof. Claudia Eckert erhält höchste Auszeichnung der TUM, die Heinz Maier-Leibnitz-Medaille
  Dec 13, 2023
- Die Lehrveranstaltungsplanung für das SS 2024 ist noch nicht abgeschlossen
  Oct 11, 2023
- Preis für gute Lehre: Claudia Eckert ausgezeichnet
  Apr 28, 2023
- Experience Cybersecurity @ Fraunhofer AISEC
  Apr 21, 2023
- Wir suchen ab sofort 1 wissenschaftliche Mitarbeiter/innen für ein Projekt zusammen mit SAP
  Mar 21, 2023

More news…