Hardware-aided Trusted Computing devroom

01.02.2x20

Overview

Trusted Execution Environments (TEEs):

- Intel SGX
- AMD SEV
- Arm TrustZone

Topics:

- Programming frameworks for TEEs
- System support for TEEs
- Use cases and applications on top of TEEs
- TEE-specific attacks and defences
- Open-source TEE architecture designs
- Vision: Future TEEs

Agenda

Submission statistics:

- Total (8), Accepted (7), Confirmed (6)
- Presentation (5), Demo (1)
- SGX (5), Arm (1)

Schedule:

10:40 – 11:15 Be secure with Rust & Intel SGX (Jethro G. Beekman)

11:20 – 11:55 The Confidential Consortium Framework (Amaury Chamayou)

12:00 – 12:35 *E*Actors: an actor-based programming framework for Intel SGX (V. A. Sartakov)

12:40 – 13:15 A Tale of Two Worlds: Assessing the Vulnerability of Enclave Shielding Runtimes (Jo Van Bulck)

13:20 – 13:55 HOWTO build a product with OP-TEE (Rouven Czerwinski)

14:00 – 14:30 Demo: SGX-LKL (Thiago Zagatti)