FDTC 2020: Final Program

FDTC 2020 is a Virtual Conference run as a Webinar (via Zoom)

Schedule is referred to Central European Summer Time (CEST)

Start: 13:00 CEST (7:00 am in New York – 8:00 pm in Tokyo)

13:00 – 13:05 Opening remarks

Keynote Talk

Chair: Guido Bertoni

13:05 – 13:55 Faulting Hardware from Software, ***Daniel Gruss****, Graz University of Technology*

Fault attacks induce misbehavior in a system, thereby possibly compromising the entire system and disclosing confidential data. Traditionally, fault attacks required hardware equipment and local access. In the past five years, some fault attacks have been discovered that require no local access and can instead be mounted from software. We first discuss the Rowhammer attack and how it can subvert a system. We then show that a new primitive, *Plundervolt*, can similarly lead to system compromise and information disclosure.

Daniel Gruss is Assistant Professor at the Graz University of Technology. He finished his PhD with honors in less than three years. Since 2010, he has been involved in teaching undergraduate courses on operating systems. His research focuses on side channels and security on the hardware-software boundary. His research team was involved in several vulnerability disclosures, including Meltdown and Spectre. Over the past five years, he has co-authored more than 20 top-tier academic publications and has received numerous awards for his research.

13:55 – 14:00 Break

Session 1 – Multi-Fault Attacks

Chair: Colin O'Flynn

14:00 – 14:25 An End-to-End Approach for Multi-Fault Attack Vulnerability Assessment
Vincent Werner*, Laurent Maingault and Marie-Laure Potet*

14:25 – 14:50 Countermeasures Optimization in Multiple Fault-Injection Context
Etienne Boespflug*, Cristian Ene, Laurent Mounier and Marie-Laure Potet*

14:50 – 15:15 SPFA: SFA on Multiple Persistent Faults
Susanne Engels*, Falk Schellenberg and Christof Paar*

15:15 – 15:45 Cofee Break

Session 2 – Fault Injection on Primitives and Systems

Chair: Tim Güneysu

15:45 – 16:10	Attacking Hardware Random Number Generators in a Multi-Tenant Scenario *Yrjo Koyen, Adriaan Peetermans,* ***Vladimir Rozic*** *and Ingrid Verbauwhede*
16:10 – 16:35	Single-bit Laser Fault Model in NOR Flash Memories: Analysis and Exploitation ***Menu Alexandre****, Jean-Max Dutertre, Jean-Baptiste Rigaud, Jean-Luc Danger, Brice Colombier and Pierre-Alain Moëllic*
16:35 – 17:00	Trouble at the CSIDH: Protecting CSIDH with Dummy-Operations against Fault Injection Attacks ***Fabio Campos****, Matthias J. Kannwischer, Michael Meyer, Hiroshi Onuki and Marc Stöttinger*
17:00 – 17:25	SiliconToaster: A Cheap and Programmable EM Injector for Extracting Secrets ***Karim Abdellatif*** *and* ***Olivier Hériveaux***
17:25 – 17:30	Closing remarks and Farewell