2.2 Physical Attacks

Date: Tuesday, March 26, 2019
Time: 11:30 - 13:00
Location / **Room:** Room 2

Chair:
Lejla Batina, Radboud University, NL, Contact Lejla Batina

Co-Chair:
Elif Kavun, University of Sheffield, GB, Contact Elif Kavun

This session covers state of the art fault analysis techniques such as persistent fault analysis, electromagnetic fault injection, and glitching. In addition, a practical attack is described on a very popular platform together with its corresponding countermeasure. Other topics in this session include the reconfigurability of FPGAs to defend against side-channel attacks and spying on IoT devices' temperature via DRAM.

Time	Label	Presentation Title Authors
11:30	2.2.1	**ONE FAULT IS ALL IT NEEDS: BREAKING HIGHER-ORDER MASKING WITH PERSISTENT FAULT ANALYSIS** **Speaker**: Shivam Bhasin, Nanyang Technological University, SG **Authors**: Jingyu Pan[1], Shivam Bhasin[2], Fan Zhang[3] and Kui Ren[3] [1]Nanyang Technological University, Zhejiang University, CN; [2]Nanyang Technological University, SG; [3]Zhejiang University, CN ***Abstract*** *Persistent fault analysis (PFA) was proposed at CHES 2018 as a novel fault analysis technique. It was shown to completely defeat standard redundancy based countermeasure against fault analysis. In this work, we investigate the security of masking schemes against PFA. We show that with only one fault injection, masking countermeasures can be broken at any masking order. The study is performed on publicly available implementations of masking.* Download Paper (PDF; Only available from the DATE venue WiFi)
12:00	2.2.2	**MULTI-TENANT FPGA-BASED RECONFIGURABLE SYSTEMS: ATTACKS AND DEFENSES** **Speaker**: Rana Elnaggar, Duke University, US **Authors**: Rana Elnaggar[1], Ramesh Karri[2] and Krishnendu Chakrabarty[1] [1]Duke University, US; [2]NYU, US ***Abstract*** *Partial reconfiguration of FPGAs improves system performance, increases utilization of hardware resources, and enables run-time update of system capabilities. However, the sharing of FPGA resources among various tenants presents security risks that affect the privacy and reliability of tenant applications running in the FPGA-based system. In this study, we examine the security ramifications of co-tenancy with a focus on address-redirection and task-hiding attacks. We design a countermeasure that protects FPGA-based systems against such attacks and prove that it resists these attacks. We present simulation results and an experimental demonstration using a Xilinx FPGA board to highlight the effectiveness of the countermeasure. The proposed countermeasure incurs negligible cost in terms of the area utilization of FPGAs currently used in the cloud.* Download Paper (PDF; Only available from the DATE venue WiFi)
12:30	2.2.3	**SPYING ON TEMPERATURE USING DRAM** **Speaker**: Nikolaos Athanasios Anagnostopoulos, TU Darmstadt, DE **Authors**: Wenjie Xiong[1], Nikolaos Athanasios Anagnostopoulos[2], André Schaller[2], Stefan Katzenbeisser[2] and Jakub Szefer[1] [1]Yale University, US; [2]Technische Universität Darmstadt, DE ***Abstract*** *Today's ubiquitous IoT devices make spying on, and collecting data from, unsuspecting users possible. This paper shows a new attack where DRAM modules, widely used in IoT devices, can be abused to measure the temperature in the vicinity of the device in order to spy on a user's behavior. Specifically, the temperature dependency of the DRAM decay is used as a proxy for user's behavior in the vicinity of the device. The attack can be performed remotely by only changing the software of an IoT device, without requiring hardware changes, and with a resolution reaching 0.5 Celsius degree. Potential defenses to the temperature spying attack are presented in this paper as well.* Download Paper (PDF; Only available from the DATE venue WiFi)
12:45	2.2.4	**MITIGATING POWER SUPPLY GLITCH BASED FAULT ATTACKS WITH FAST ALL-DIGITAL CLOCK MODULATION CIRCUIT** **Speaker**: Nikhil Chawla, Georgia Institute of Technology, US **Authors**: Arvind Singh[1], Monodeep Kar[2], Nikhil Chawla[1] and Saibal Mukhopadhyay[1] [1]Georgia Institute of Technology, US; [2]Intel Corporation, US ***Abstract*** *This paper experimentally demonstrates that an on-chip integrated fast all-digital clock modulation (F-ADCM) circuit can be used as a countermeasure against supply glitch and temperature variations-based fault injection attacks (FIA). The F-ADCM circuit modulates clock edges in presence of DC/transient supply glitches and temperature variations to ensure correct operation of the underlying cryptographic circuit. With a testchip manufactured in 130nm CMOS process, we first demonstrate an inexpensive methodology to conduct a fault attack on hardware implementation of a 128-bit advanced encryption standard (AES) engine using externally controlled supply glitches. Next, we show that with F-ADCM circuit, it is no longer possible to inject supply/temperature glitch-based faults even after 10 million encryptions across varying operating conditions. Moreover, in extreme operating conditions, the F-ADCM circuit doesn't generate any clock edges, leading to complete failure of the AES encryption, indicating no exploitable faults are present.* Download Paper (PDF; Only available from the DATE venue WiFi)

Time	Label	Presentation Title Authors
13:00	IP1-1, 384	**FAULT INJECTION ON HIDDEN REGISTERS IN A RISC-V ROCKET PROCESSOR AND SOFTWARE COUNTERMEASURES** **Speaker**: Johan Laurent, Univ. Grenoble Alpes, Grenoble INP, LCIS, FR **Authors**: Johan Laurent[1], Vincent Beroulle[1], Christophe Deleuze[1] and Florian Pebay-Peyroula[2] [1]LCIS - Grenoble Institute of Technology - Univ. Grenoble Alpes, FR; [2]CEA-Leti, FR ***Abstract*** *To protect against hardware fault attacks, developers can use software countermeasures. They are generally designed to thwart software fault models such as instruction skip or memory corruption. However, these typical models do not take into account the actual implementation of a processor. By analyzing the processor microarchitecture, it is possible to bypass typical software countermeasures. In this paper, we analyze the vulnerability of a secure code from FISSC (Fault Injection and Simulation Secure Collection), by simulating fault injections in a RISC-V Rocket processor RTL description. We highlight the importance of hidden registers in the processor pipeline, which temporarily hold data during code execution. Secret data can be leaked by attacking these hidden registers. Software countermeasures against such attacks are also proposed.* Download Paper (PDF; Only available from the DATE venue WiFi)
13:01	IP1-2, 476	**METHODOLOGY FOR EM FAULT INJECTION: CHARGE-BASED FAULT MODEL** **Speaker**: Haohao Liao, University of Waterloo, CA **Authors**: Haohao Liao and Catherine Gebotys, University of Waterloo, CA ***Abstract*** *Recently electromagnetic fault injection (EMFI) techniques have been found to have significant implications on the security of embedded devices. Unfortunately there is still a lack of understanding of EM fault models and countermeasures for embedded processors. For the first time, this paper proposes an extended fault model based on the concept of critical charge and a new EMFI backside methodology based on over-clocking. Results show that exact timing of EM pulses can provide reliable repeatable instruction replacement faults for specific programs. An attack on AES is demonstrated showing that the EM fault injection requires on average less than 222 EM pulses and 5.3 plaintexts to retrieve the full AES key. This research is critical for ensuring embedded processors and their instruction set architectures are secure and resistant to fault injection attacks.* Download Paper (PDF; Only available from the DATE venue WiFi)
13:02	IP1-3, 807	**SECURING CRYPTOGRAPHIC CIRCUITS BY EXPLOITING IMPLEMENTATION DIVERSITY AND PARTIAL RECONFIGURATION ON FPGAS** **Speaker**: Benjamin Hettwer, Robert Bosch GmbH, DE **Authors**: Benjamin Hettwer[1], Johannes Petersen[2], Stefan Gehrer[1], Heike Neumann[2] and Tim Güneysu[3] [1]Robert Bosch GmbH, Corporate Sector Research, DE; [2]Hamburg University of Applied Sciences, DE; [3]Horst Görtz Institute for IT Security, Ruhr-University Bochum, DE ***Abstract*** *Adaptive and reconfigurable systems such as Field Programmable Gate Arrays (FPGAs) play an integral part of many complex embedded platforms. This implies the capability to perform runtime changes to hardware circuits on demand. In this work, we make use of this feature to propose a novel countermeasure against physical attacks of cryptographic implementations. In particular, we leverage exploration of the implementation space on FPGAs to create various circuits with different hardware layouts from a single design of the Advanced Encryption Standard (AES), that are dynamically exchanged during device operation. We provide evidence from practical experiments based on a modern Xilinx ZYNQ UltraScale+ FPGA that our approach increases the resistance against physical attacks by at least factor two. Furthermore, the genericness of our approach allows an easy adaption to other algorithms and combination with other countermeasures* Download Paper (PDF; Only available from the DATE venue WiFi)
13:03	IP1-4, 367	**STT-ANGIE: ASYNCHRONOUS TRUE RANDOM NUMBER GENERATOR USING STT-MTJ** **Speaker**: Ben Perach, Faculty of Electrical Engineering. Technion - Israel Institute of Technology, IL **Authors**: Ben Perach and Shahar Kvatinsky, Technion, IL ***Abstract*** *The Spin Transfer Torque Magnetic Tunnel Junction (STT-MTJ) is an emerging memory technology whose interesting stochastic behavior might benefit security applications. In this paper, we leverage this stochastic behavior to construct a true random number generator (TRNG), the basic module in the process of encryption key generation. Our proposed TRNG operates asynchronously and thus can use small and fast STT MTJ devices. As such, it can be embedded in low-power and low-frequency devices without loss of entropy. We evaluate the proposed TRNG using a numerical simulation, solving the Landau-Lifshitz-Gilbert (LLG) equation system of the STTMTJ devices. Design considerations, attack analysis, and process variation are discussed and evaluated. The evaluation shows that our solution is robust to process variation, achieving a Shannon-entropy generating rate between 99.7Mbps and 127.8Mbps for 90% of the instances.* Download Paper (PDF; Only available from the DATE venue WiFi)

Time	Label	Presentation Title Authors
13:00		End of session **Lunch Break** in Lunch Area

Coffee Breaks in the Exhibition Area

On all conference days (Tuesday to Thursday), coffee and tea will be served during the coffee breaks at the below-mentioned times in the exhibition area.

Lunch Breaks (Lunch Area)

On all conference days (Tuesday to Thursday), a seated lunch (lunch buffet) will be offered in the Lunch Area to fully registered conference delegates only. There will be badge control at the entrance to the lunch break area.

Tuesday, March 26, 2019

- Coffee Break 10:30 - 11:30
- Lunch Break 13:00 - 14:30
- Keynote Lecture "Leonardo da Vinci, Humanism and Engineering between Florence and Milan" by Claudio Giorgione in room 1 13:50 - 14:20
- Coffee Break 16:00 - 17:00

Wednesday, March 27, 2019

- Coffee Break 10:00 - 11:00
- Lunch Break 12:30 - 14:30
- Keynote Lecture "Heterogeneous, High Scale Computing in the Era of Intelligent, Cloud-Connected" by David Pellerin, Amazon, US in room 1 13:50 - 14:20
- Coffee Break 16:00 - 17:00

Thursday, March 28, 2019

- Coffee Break 10:00 - 11:00
- University Booth Best Demo Award Presentation at the University Booth 10:30
- Lunch Break 12:30 - 14:00
- Keynote Lecture "A Fundamental Look at Models and Intelligence" by Edward A. Lee, University of California, Berkeley, US in room 1 13:20 - 13:50
- Coffee Break 15:30 - 16:00