W05 Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE 2018)

Hardware security is becoming increasingly important for many embedded systems applications, ranging from small RFID tags to satellites orbiting the earth. The number of secure applications, such as public services, communication and healthcare, keeps on growing. Hardware devices that implement cryptography functions have become the Achilles’ heel of these systems.

The TRUDEVICE Workshop will provide an environment for researchers from academic and industrial domains who want to discuss recent findings, theories and on-going work on all aspects of hardware security including design, manufacturing, testing, reliability, validation and utilization.

The topics of the workshop include:

- Manufacturing Test of Secure Devices
- Trustworthy Manufacturing of Secure Devices
- PUFs and TRNGs
- Hardware Trojans in IPs and ICs
- Reconfigurable Devices for Security
- Fault Attack Injection, Detection and Protection
- Validation and Evaluation Methodologies for Physical Security
- Side Channel Attacks and Countermeasures

Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Label</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:30</td>
<td>W05.1</td>
<td>Session 1: Physical attacks</td>
</tr>
<tr>
<td>08:30</td>
<td>W05.1.1</td>
<td>Keynote 1</td>
</tr>
<tr>
<td>09:30</td>
<td>W05.1.2</td>
<td>Automatic Application of Side Channel Countermeasures: History and Perspectives</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Francesco Regazzoni, AlaRI, CH</td>
</tr>
<tr>
<td>10:00</td>
<td>W05.2</td>
<td>Poster Session 1 + Coffee Break</td>
</tr>
<tr>
<td>10:00</td>
<td>W05.2.1</td>
<td>Dummy rounds side-channel attack protection of round-based encryption algorithms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stanislav Jerabek, Jan Schmidt and Martin Novotny, CTU, CZ</td>
</tr>
<tr>
<td>10:00</td>
<td>W05.2.2</td>
<td>A New Metric for the Side-Channel Vulnerability Evaluation?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Jan Bělohloubek, Petr Fiser and Jan Schmidt, CTU, CZ</td>
</tr>
<tr>
<td>10:00</td>
<td>W05.2.3</td>
<td>Influence of Fault-Tolerance Techniques on Power-Analysis Resistance of AES implemented in FPGA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vojtěch Mákevský, Hana Kubatova and Martin Novotny, CTU, CZ</td>
</tr>
<tr>
<td>10:30</td>
<td>W05.3</td>
<td>Session 2: Active attacks and systems integrity</td>
</tr>
</tbody>
</table>
10:30 W05.3.1 A Hybrid Approach for Ensuring the Security of Hardware Control Systems
Naceur Maha, Ulrich Kuehne and Jean-Luc Danger, Télécom ParisTech, FR

11:00 W05.3.2 On Security Metrics for Evaluating Fault-Injection Countermeasures
Mael Gay¹, Batya Kap², Osnat Karen² and Ilia Polian³
¹University of Passau, DE; ²Bar-Ilan University, IL; ³University of Stuttgart, DE

11:30 W05.3.3 SCA & Glitch Rogue: An Accurate Side Channel Analysis and Glitch Attack Evaluation Platform for Embedded Systems
Athanasios Papadimitriou and David Hely, Univ. Grenoble Alpes, FR

11:45 W05.3.4 Nonlinear Codes for Control Flow Checking
Giorgio Di Natale¹ and Osnat Keren²
¹LIRMM, FR; ²Bar-Ilan University, IL

12:00 W05.4 Lunch Break

13:00 W05.5 Session 3: Design and test of secure hardware

13:00 W05.5.1 Keynote 2

14:00 W05.5.2 Does stream cipher-based scan chains encryption really prevent scan attacks?
Matheiu Da Silva, Marie-Lise Fortes, Giorgio Di Natale and Bruno Rouzeyre, LIRMM, FR

14:30 W05.6 Poster Session 2 + Coffee Break

14:30 W05.6.1 Dynamic reconfiguration used for side channel attacks protection of various encryption algorithms
Jan Brejnik, Stanislav Jerabek and Martin Novotny, CTU, CZ

14:30 W05.6.2 Xilinx 7-Series FPGA Based Evaluation Platform for Physically Unclonable Function
Matej Bartík, CTU, CZ

15:00 W05.7 Session 4: Hardware circuit security

15:00 W05.7.1 Using Convolutional Codes for Key Extraction in SRAM Physical Unclonable Functions
Sven Mueellich, Sven Puchinger and Martin Bossert, Ulm University, DE

15:30 W05.7.2 Towards Inter-Vendor Compatibility of TRNGs for FPGAs
Milos Gujic¹, Bohan Yang¹, Vladimir Roz¹ and Ingrid Verbauwhede²
¹KU Leuven, BE; ²KU Leuven and UCLA, BE

16:00 W05.7.3 Two Methods of the Clock Jitter Measurement Aimed at Embedded TRNG testing
Oto Petura¹, Marek Laban², Elie Noumon Ali² and Viktor Fischer³
¹Hubert Curien Laboratory, Jean Monnet University, FR; ²Technical University of Kosice, SK; ³Jean Monnet University Saint-Etienne, FR; ⁴Laboratoire Hubert Curien, FR

16:15 W05.7.4 Random Bit Generation Based on The Association of Serial CBRAM Devices
Daniel Arum, Salvador Manich and Rosa Rodriguez, UPC, ES

16:30 W05.7.5 Hardware Trojan Detection and Obfuscation based on Approximate Circuits
Hernesto Martin¹, Giorgio Di Natale², Sophie Dupuis² and Luis Entrena¹
¹University Carlos III de Madrid, ES; ²LIRMM, FR

16:45 W05.7.6 Using different LUT paths to increase area efficiency of RO-PUFs on Altera FPGAs
Linus Feiten, Karsten Scheibler, Bernd Becker and Matthias Sauer, University of Freiburg, DE

Source URL: https://www.date-conference.com/date18/conference/workshop-w05

Links:
[1] https://www.date-conference.com/date18/user/1157/contact_form
[2] https://www.date-conference.com/date18/user/21993/contact_form
[3] https://www.date-conference.com/date18/user/22198/contact_form
[4] https://www.date-conference.com/date18/user/22039/contact_form
[5] https://www.date-conference.com/date18/user/1041/contact_form
[6] https://www.date-conference.com/date18/user/25193/contact_form
[7] https://www.date-conference.com/date18/user/24477/contact_form
[8] https://www.date-conference.com/date18/user/3369/contact_form
[9] https://www.date-conference.com/date18/user/1156/contact_form
[10] https://www.date-conference.com/date18/user/25339/contact_form
[12] https://www.date-conference.com/date18/user/77174/contact_form
[13] https://www.date-conference.com/date18/user/17365/contact_form
[14] https://www.date-conference.com/date18/user/936/contact_form
[15] https://www.date-conference.com/date18/user/58795/contact_form
[16] https://www.date-conference.com/date18/user/3920/contact_form