Call for Contributions for SCADD

Note: Onsite and Online Options
In order to accommodate a large number of situations, we are offering the option for either physical presence or virtual participation. We would be delighted if all authors manage to attend in person, but are aware that special circumstances are best handled by having flexible options.

Submission:
1. Inform the Chair: with the Title of your Contribution
2. Submission URL:
https://www.iariasubmit.org/conferences/submit/newcontribution.php?event=CYBER+2020+Special
Please select Track Preference as **SCADD**

Special track

SCADD: Side Channel Attacks, Detection & Defenses

Chairs and Coordinators

Dr. Khurram Bhatti, Associate Professor, Information Technology University (ITU), Lahore, Pakistan
Khurram.bhatti@itu.edu.pk
Dr. Maria Mushtaq, Scientific Researcher, LIRMM –CNRS, University of Montpellier, France
maria.mushtaq@lirmm.fr

along with

CYBER 2020, The Fifth International Conference on Cyber-Technologies and Cyber-Systems
https://www.iaria.org/conferences2020/CYBER20.html
October 25-29, 2020 - Nice, French Riviera, France

Cyber security has become an encompassing term that is succinct, but expresses the breadth of coverage across multiple overlapping domains. Security is a system-wide issue and modern computing systems need to take a holistic approach to the design, development, and deployment of security solutions. The revelations of security and privacy vulnerabilities in microprocessors over the past few years, both at hardware and software level, have been appalling. These vulnerabilities affect almost every processor, across virtually every operating system and architecture.

In recent years, researchers have demonstrated that modern computing systems are vulnerable both from computational as well as storage perspectives and most of the performance optimizations present in modern-day computing systems can potentially expose them to adversary and leak critical information. These existing vulnerabilities lead to side-channel information leakage in many different ways, such as: variation in physical parameters like power consumption, electromagnetic radiation and acoustic emanation as well as logical parameters like memory access pattern, access timing and fault occurrences. Moreover, new leakage channels keep appearing in existing architectures. Thus, the real attack surface is unknown, both at the software level and at the hardware level. Side-channel analysis (SCA) has, therefore, become an important field of research. Side-channel attacks exploit existing vulnerabilities to extract privileged information both at computational and storage levels. In order to enhance the resistance of cryptographic and security critical implementations within the design phase, constructive attacks and analysis techniques may serve as a quality metric to optimize the design and development process.

SCADD special track at the CYBER-2020 conference will provide an international platform for researchers, academics, and industry participants to present their work and their current research topics.

The topics include, but are not limited to the following subtopics:

1. **Attacks and exploitations**

Side-channel analysis, fault-injection attacks, probing and read-out, hardware Trojans, cloning and counterfeiting, side-channel or fault-injection based reverse engineering

2. **Secure implementation**

Cryptographic blocks (including post-quantum and lightweight ciphers), random number generators, physical unclonable functions, leakage-resilient cryptography, fault-injection tolerant design, and tamper-detection

3. **Implementation attack-resilient architectures and schemes**

Trusted environment (Secure boot, execution, storage, isolation, virtualization, firmware update), protections against micro-architectural side-channels and covert channels, cache attacks, software-enabled implementation attacks, white-box cryptography

4. **Secure design and evaluation**

Security and leakage models, formal analysis of secure implementations, design automation and tools, evaluation tooling, domain-specific security analysis of e.g., IoT, medical, automotive, industrial-control systems, mobile, security analysis based on artificial intelligence

5. **Practical attacks, test platforms and open benchmarks**

Practical implementation of physical attacks, practical demonstrators of Trojan insertion, test platforms for evaluation of physical attacks, open benchmarks for hardware Trojans, physical attacks and countermeasures.

6. **Detection Techniques**

Run-time detection techniques, machine learning based detection techniques, attack surface assessment techniques

7. **Countermeasure Techniques**

Formal methods for design phase countermeasures, run-time countermeasures, operating system and hypervisor level countermeasures, hardware countermeasures, countermeasures at cache and memory hierarchy, isolation-based techniques, trusted environment.

Important Datelines

Inform the Chair: As soon as you decide to contribute
Submission: August 1, 2020
Notification: August 21, 2020
Registration: September 1, 2020
Camera-ready: September 1, 2020

Note: *These deadlines are somewhat flexible, providing arrangements are made ahead of time with the chair.*

Contribution Types

- Regular papers [in the proceedings, digital library]
- Short papers (work in progress) [in the proceedings, digital library]
- Posters: two pages [in the proceedings, digital library]
- Posters: slide only [slide-deck posted on www.iaria.org]
- Presentations: slide only [slide-deck posted on www.iaria.org]
- Demos: two pages [posted on www.iaria.org]

Paper Format

- See: http://www.iaria.org/format.html [both LaTex and .doc templates]
- Before submission, please check and comply with the editorial rules: http://www.iaria.org/editorialrules.html
- More information on camera ready preparations will be posted after the paper notifications are sent out.

Publications

- Extended versions of selected papers will be published in IARIA Journals: http://www.iariajournals.org
- Print proceedings will be available via Curran Associates, Inc.: http://www.proceedings.com/9769.html
- Articles will be archived in the free access ThinkMind Digital Library: http://www.thinkmind.org

Paper Submission

https://www.iariasubmit.org/conferences/submit/newcontribution.php?event=CYBER+2020+Special
Please select Track Preference as **SCADD**

Registration

- Each accepted paper needs at least one full registration, before the camera-ready manuscript can be included in the proceedings.
- Registration fees are available at http://www.iaria.org/registration.html

Contacts

Khurram Bhatti: Khurram.bhatti@itu.edu.pk
Maria Mushtaq: maria.mushtaq@lirmm.fr
CYBER Logistics: steve@iaria.org
