IEEE CSR 2025
Cyber Security and Resilience

Chania, Crete, Greece | August 4–6, 2025

https://www.ieee-csr.org

# 2025 IEEE CSR Workshop on Hardware Cybersecurity Systems (HACS)

## Call for Papers

### Important dates

Paper submission deadline:
**May 5, 2025**
Authors' notification:
**May 26, 2025**
Camera-ready submission:
**June 16, 2025**
Registration deadline (authors):
**June 16, 2025**
Workshop dates:
**August 4–6, 2025**

### Workshop chairs

Peter Langendoerfer (DE)
Christophe Bobda (US)
Nicolas Sklavos (GR)

### Technical program committee

Giovanni Agosta (IT)
Ricardo Chaves (PT)
Pascal Cotret (FR)
Soumyajit Dey (IN)
Giorgio Di Natale (FR)
Zoya Dyka (DE)
Aurelien Francillion (FR)
Basel Halak (UK)
Ivgen Kabin (DE)
Elif Bilge Kavun (DE)
Paris Kitsos (GR)
Dominik Klein (DE)
Nicholas Kolokotronis (GR)
Ulrich Kühne (FR)
Marco Macchetti (CH)
Yiorgos Makris (US)
Vincent Mooney (US)
Maria Mushtaq (FR)
Francesco Regazzoni (CH)
Vincent Rijmen (BE)
Ioannis Savidis (US)
Georgios Selimis (NL)
Anirban Sengupta (IN)
Dimitrios Serpanos (GR)
Stavros Shiaeles (UK)
Leonel Sousa (PT)
Sara Tehranipoor (US)
Guzin Ulutas (TR)
Sherali Zeadally (US)
Mark Zwolinski (UK)

### Publicity chairs

Peter Langendoerfer (DE)

### Contact us

peter.langendoerfer@b-tu.de

Resilience of the Internet of Things, industrial control systems, critical infrastructures and health care etc. is of utmost importance. The basis to achieve this are trustworthy embedded devices. In order to ensure trustworthiness of these devices their whole life cycle needs to be taken into account. This means their design, production, deployment and use. Here considering hardware and embedded software such as operating systems and firmware. Computing hardware has become an attractive attack surface, either due to unintentional design flaws or malicious design modifications. Hardware designers and automation tool developers alike are challenged to understand the different hardware security threats in order to incorporate effective countermeasures into robust hardware design, verification, and testing. This holds true not only for security-related hardware components but also for general-purpose processors. The most common targets in such adversary attacks are secure architectures, cryptographic primitives, and intellectual property (IP) by counterfeiting. Well-known hardware security threats are e.g. Hardware Trojans (HT), Reverse Engineering (RE), covert and side channels. In addition continuously advancing, novel attacks targeting remote, cross-layer liabilities also become prevalent. In order to ensure trustworthiness of embedded systems also the embedded GPUs need to support secure processing by e.g. providing means to ensure control flow integrity. In addition, operating systems and firmware need to be hardened to reduce vulnerabilities related to known attack types such as buffer overflows and return-oriented-programming, return-to-libc etc. But also AI based attack detection means, implemented in hard- or software, are required to detect novel, innovative attacks during the normal operation of the devices.

The workshop will be held in conjunction with the IEEE CSR 2025 conference as a **physical event**, during August 4–6, 2025. Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include but are not limited to the following:

- Architectures and applications: 5G/6G, healthcare, IoT, etc.
- Networks, protocols and communications: hardware integrations
- Attacks: implementations and countermeasures
- Constrained and trusted environments
- Cryptanalysis/Side channel attacks for hardware
- Cryptographic primitives and lightweight cryptography
- Hardware obfuscation
- Hardware crypto-processors, system-on-chip (SoC) and reconfigurable designs
- Trust and anti-counterfeiting
- Reverse engineering, Hardware Trojans detection and countermeasures
- Attack detection: Control flow integrity, AI based attack detection etc.
- Software life cycle integrity
- Secure, trustworthy operating systems and firmware

The IEEE CSR HACS workshop will accept high-quality research papers presenting strong theoretical contributions, applied research and innovation results obtained from funded cyber-security and resilience projects, and industrial papers that promote contributions on technology development and contemporary implementations.

Submitted manuscripts should not exceed 6 pages (plus 2 extra pages, being subject to overlength page charges) and should be of sufficient detail to be evaluated by expert reviewers in the field. Accepted papers will be submitted for inclusion into IEEE Xplore subject to meeting IEEE Xplore's scope and quality requirements. Detailed information about paper submission and guidelines for authors can be found at the workshop's website https://www.ieee-csr.org/hacs.

IEEE
IEEE SMC Systems, Man, and Cybernetics Society
SMC Homeland Security Technical Committee
LOGOS RI RESEARCH&INNOVATION