Call for Papers

Important dates

Paper submission deadline:
June 3, 2024 AoE
Authors' notification:
July 3, 2024 AoE
Camera-ready submission:
July 14, 2024 AoE
Early registration deadline:
July 20, 2024 AoE
Workshop dates:
September 2–4, 2024

Workshop chairs

Nicolas Sklavos (GR)
Valeria Loscri (FR)

Technical program committee

Giovanni Agosta (IT)
Allesandro Brighente (IT)
Ileana Buhan (NL)
Ricardo Chaves (PT)
Pascal Cotret (FR)
Soumyajit Dey (IN)
Giorgio Di Natale (FR)
Zoya Dyka (DE)
Alexander Fish (IL)
Apostolos Fournaris (GR)
Basel Halak (UK)
Ivgen Kabin (DE)
Elif Bilge Kavun (DE)
Osnat Keren (IL)
Paris Kitsos (GR)
Odysseas Koufopavlou (GR)
Ulrich Kühne (FR)
Peter Langendoerfer (DE)
Francesco Leporati (IT)
Alla Levina (RU)
Marco Macchetti (CH)
Nikolay Moldovyan (RU)
Maria Mushtaq (FR)
Francesco Regazzoni (NL/CH)
Vincent Rijmen (BE/NO)
Georgios Selimis (NL)
Stavros Shiales (UK)
Leonel Sousa (PT)
Sara Tehranipoor (US)
Guzin Ulutas (TR)
Selma Yahia (FR)
Sherali Zeadally (US)

Contact us

nsklavos@upatras.gr

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. The most common targets in such adversary attacks are secure architectures, cryptographic primitives, and intellectual property (IP) by counterfeiting. Moreover, as increasingly more Internet of Things (IoT) applications are emerging, vulnerabilities to cyberattacks are created as well, with new hardware-based defense mechanisms for smart systems and devices being in need. With well-known hardware security threats such as Hardware Trojans (HT), Reverse Engineering (RE), and covert and side channels continuously advancing, novel attacks targeting remote, cross-layer liabilities also become prevalent.

At the same time, hardware solutions have proven to be highly efficient when it comes to security assurance. Two such security primitives are True Random Number Generators (TRNGs) and Physical Unclonable Functions (PUFs), which offer protection against spoofing and tampering attacks. Lightweight cryptographic modules are especially useful as an increasing number of devices in the IoT with resource constraints require strong security and mutual authentication schemes. Hardware implementation of cryptographic primitives can offer flexibility, power efficiency, and the ability of parallel processing. Since the physical layer often acts as the base of trust in a system, a promising research direction towards state-of-the-art hardware security solutions is being formed.

The workshop is held in conjunction with the IEEE CSR 2024 conference as a **hybrid event**, during September 2–4, 2024. 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.
- Attacks: implementations and countermeasures
- Constrained and trusted environments
- Cryptanalysis for hardware
- Cryptographic primitives and lightweight cryptography
- Hardware obfuscation
- Hardware crypto-processors, system-on-chip (SoC) and reconfigurable designs
- Networks, protocols and communications: hardware integrations
- PUFs, trojans and TRNGs on hardware
- Reverse engineering
- Smart cards cybersecurity
- Trust and anti-counterfeiting

The 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