Important dates

Paper submission deadline:
March 15, 2023
Authors' notification:
April 01, 2023
Camera-ready submission:
April 15, 2023
Early registration deadline:
May 5, 2023
HYBRID EVENT

General Chair
Nicolas Sklavos

Organizing Committee
Paris Kitsos
Odysseas Koufopavlou
Valeria Loscri
Ivana Ognjanovic
Nicolas Sklavos
Sherali Zeadally

Publicity Chair
Paris Kitsos

Program Committee
Soumyajit Dey
Zoya Dyka
Basel Halak
Ievgen Kabin
Cetin Kaya Koc
Ulrich Kühne
Peter Langendörfer
Francesco Leporati
Nikolay A. Moldovyan
Maria Mushtaq
Giorgio Di Natale
Josef Pieprzyk
Francesco Regazzoni
Vincent Rijmen
Georgios Selimis
Stavros Shiaeles
Leonel Sousa
Sara Tehranipoor

Contact
Nicolas Sklavos,
e-mail: nsklavos@upatras.gr

Call for Papers

IEEE Workshop on Hardware Cybersecurity Systems (HACS)

Scope

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 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.

Related areas, in alphabetical order, include but are not limited to:

- *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
- Networks, Protocols and Communications: Hardware Integrations
- PUFs, Trojans and TRNGs on Hardware
- Reverse Engineering
- Smart Cards Cybersecurity
- *Trust and Anti-Counterfeiting*

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