ASHES 2019 – CALL FOR PAPERS & PARTICIPATION

We are happy to announce the **Third Workshop on Attacks and Solutions in Hardware Security (ASHES 2019)**, a post-conference workshop of **ACM CCS 2019**, one of the premier computer security conferences, in London, UK.

ASHES deals with any aspects of hardware security, and welcomes any contributions in this area. Among others, it particularly highlights emerging techniques and methods as well as recent application areas within the field. This includes new attack vectors, novel designs and materials, lightweight security primitives, nanotechnology, and PUFs on the methodological side, as well as the internet of things, automotive security, smart homes, pervasive and wearable computing on the applications side.

Specific topics of interest include, but are not limited to:

- Fault injection, side channels, hardware Trojans, and countermeasures
- Tamper sensing and tamper protection
- New physical attack vectors or methods
- Biometrics
- Secure sensors
- Device fingerprinting and hardware forensics
- Lightweight hardware solutions
- Secure, efficient, and lightweight hardware implementations
- Security of reconfigurable and adaptive hardware
- Emerging computing technologies in security
- New designs and materials in hardware security
- Nanophysics and nanotechnology in hardware security
- PUFs and new/emerging variants thereof
- Item tagging, secure supply chains, and product piracy
- Intellectual property protection and content protection
- Scalable hardware solutions for many players/endpoints
- Hardware security and machine learning
- Hardware security in emerging application scenarios
- Architectural factors and hardware security in the cloud
- Electronic voting machines
- Nuclear weapons inspections and arms control
- Physical layer and wireless network security
- Anti-forensic attacks and protection
- Mobile devices, smart cards, and chip cards
- Architectural factors in hardware security, isolation versus encryption
- Secure hardware for multiparty computation
- Integration of hardware roots of trust and PUFs
- Quality metrics for secure hardware
- Conformance and evaluation of secure hardware
- Formal treatments, proofs, standardization, or categorization of hardware-related methods

To account for the special nature of hardware security as a rapidly developing discipline, **ASHES hosts four different categories of papers**: Classical **full papers**, **short papers**, **wild and crazy (WaC) papers** (whose purpose is rapid dissemination of promising, potentially game-changing novel ideas), and **systematization of knowledge (SoK) papers** (which overview, structure, and categorize a certain subarea). Please visit the workshop's website for further details: http://ashesworkshop.org/call-for-papers

The workshop will host several technical sessions and **two invited keynotes** by **Ross Anderson (Cambridge)** and **F.-X. Standaert (UC Louvain).**

Committees

Steering Committee

Chip Hong Chang (NTU, Singapore)
Srini Devadas (MIT)
Marten van Dijk (U Connecticut)
Farinaz Koushanfar (UC San Diego)
Ulrich Rührmair (LMU Munich)
Ahmad-Reza Sadeghi (TU Darmstadt)
F.-X. Standaert (UC Louvain)
Mark M. Tehranipoor (U Florida)
Ingrid Verbauwhede (KU Leuven)

Workshop Chairs

Chip Hong Chang (NTU Singapore)
Ulrich Rührmair (LMU Munich)

PC Chairs

Dan Holcomb (UMass Amherst)
Patrick Schaumont (Virginia Tech)

Proceedings Chair

Francesco Regazzoni (U Lugano)

Web Chair

Yuan Cao (Hohai U)

Important Dates

Paper submission deadline:
July 5, 2019 23:59:59 EDT

Acceptance notification:
August 7, 2019

Camera-ready deadline:
August 30, 2019

Workshop Date:
November 15, 2019

ashesworkshop.org