ASHES 2018 —
ATTACKS AND SOLUTIONS
IN HARDWARE SECURITY
Oct. 19, 2018, Toronto, CA

ASHES 2018 – CALL FOR PAPERS & PARTICIPATION

We are happy to announce the **Second Workshop on Attacks and Solutions in Hardware Security (ASHES 2018)**, a post-conference workshop of **ACM CCS 2018**, one of the premier computer security conferences, in Toronto, Canada.

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:

- Tamper sensing and tamper protection
- Physical attacks (fault injection, side-channels, etc.), including new attack vectors or attack methods
- Biometrics and hardware security
- Physical unclonable functions (and new/emerging variants thereof)
- Device fingerprinting and hardware forensics
- Item tagging, secure supply chains and product piracy
- Use of emerging computing technologies in security (including quantum techniques)
- New designs and materials for secure hardware
- Nanophysics and nanotechnology in hardware security
- Hardware Trojans and countermeasures
- Lightweight security solutions, primitives and protocols
- Secure and efficient hardware implementation of cryptographic primitives
- Security of reconfigurable and adaptive hardware platforms
- Secure sensors and sensor networks, including physical attacks and countermeasures
- Hardware security in emerging scenarios: Internet of Things, smart home, automotive and autonomous systems, wearable computing, pervasive and ubiquitous computing, etc.
- Scalable hardware solutions that work for particularly large numbers of players/endpoints
- Secure and scalable hardware implementation of machine learning algorithms
- Formal treatments, proofs, standardization, or categorization of the area (incl. surveys and systematization of knowledge papers)

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 include several technical sessions and invited keynotes, among them **Srdjan Capkun (ETH)** on general hardware security and **Alexander Glaser (Princeton)** on security aspects in nuclear weapons inspections.

Committees

Steering Committee

Chip Hong Chang (NTU, Singapore)
Srini Devadas (MIT)
Marten van Dijk (U Connecticut)
Farinaz Koushanfar (UC San Diego)
Ulrich Rührmair (U Bochum)
Mark M. Tehranipoor (U Florida)

Workshop Organizers

Chip Hong Chang (NTU Singapore)
Ulrich Rührmair (U Bochum)

PC Chairs

Jorge Guajardo (Bosch RTC)
Dan Holcomb (UMass Amherst)

Proceedings Chair

Francesco Regazzoni (U Lugano)

Web Chair

Yuan Cao (Hohai U)

Publicity and Industry Liaison Chairs

Domenic Forte (U Florida)
Sohrab Aftabjahani (Intel)

Important Dates

Paper submission deadline:
July 8, 2018 23:59:59 EDT

Acceptance notification:
August 5, 2018

Camera-ready deadline:
August 19, 2018

Workshop date:
October 19, 2018

ashesworkshop.org