ASHES '23: Workshop on Attacks and Solutions in Hardware Security

Lejla Batina
Radboud University
lejla@cs.ru.nl

Chip Hong Chang
NTU Singapore
ECHChang@ntu.edu.sg

Domenic Forte
University of Florida
dforte@ece.ufl.edu

Ulrich Rührmair
TU Berlin and U Connecticut
ruehrmair@ilo.de

ABSTRACT AND OVERVIEW

The workshop on **"Attacks and Solutions in HardwarE Security (ASHES)"** welcomes **any** theoretical and practical works on hardware security, including attacks, solutions, countermeasures, proofs, classification, formalization, and implementations. Besides mainstream research, ASHES puts some focus on new and emerging scenarios: This includes the Internet of Things (IoT), nuclear weapons inspections, arms control, consumer and infrastructure security, or supply chain security, among others. ASHES also welcomes works on special purpose hardware, such as lightweight, low-cost, and energy-efficient devices, or non-electronic security systems.

The workshop hosts four different paper categories: Apart from regular and short papers, this includes works that systematize and structure a certain (sub-)area (so-called *"Systematization of Knowledge"* (SoK) papers), and so-termed *"Wild-and-Crazy"* (WaC) papers, which distribute seminal ideas at an early conceptual stage. This summary gives a brief overview of the seventh edition of the workshop, which took place on November 30, 2023 in Copenhagen, Denmark, as a post-conference satellite workshop of ACM CCS.

CCS Concepts

• CCS Concept: Hardware Security

Keywords: Theory and practice of hardware (HW) security, HW attacks, HW solutions, HW implementations, Internet of Things (IoT), non-electronic HW

ACM Reference Format:
Lejla Batina, Chip Hong Chang, Domenic Forte, & Ulrich Rührmair. 2023. ASHES '23: Workshop on Attacks and Solutions in Hardware Security. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS'23), November 26–30, 2023, Copenhagen, Denmark.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3576915.3624028

CCS '23, November 26–30, 2023, Copenhagen, Denmark

ACM ISBN 979-8-4007-0050-7/23/11 .
https://doi.org/10.1145/3576915.3624028

1 INTRODUCTION AND MOTIVATION

As predicted by IDC, there will be around 42 billion hardware devices connected in the IoT by 2025, generating and collecting around 80 zettabytes of data every year. This makes the IoT clearly one of the most massive and impactful human endeavors of this century.

At the same time, the development of suitable hardware security strategies seems to lag behind the actual spread of the IoT. While the security community has long recognized that many of the established, classical recipes do not transfer easily (or not at all) to hardware in an IoT-setting, no fully convincing substitute strategies have been developed yet.

This leads to a host of novel and open questions, which cannot be addressed by existing means and methods alone. Particularly pressing issues in this context include:

- How can we get individual cryptographic keys into billions of low-cost hardware devices?
- How can we securely identify hardware over digital channels, including systems without digital signal processors or devices merely powered by scavenged energy?
- How can we protect against tampering and side-channels in hardware?
- How can we remotely verify the functionality and integrity of connected IoT-devices?
- How can we establish the long-term confidentiality of communications with resource-constrained hardware?
- How can we protect hardware against malware (viruses, Trojan horses, etc.) and network attacks?
- How can we enable secure physical data storage, especially in highly connected, potentially lightweight hardware systems?
- How can we preserve the privacy of users in connected systems and in pervasive IoT-scenarios?

The purpose of the ASHES workshop is to foster solutions for these and other impending issues on hardware security, including new methods and application scenarios, such as the IoT, but also many others. It shall provide the CCS-community with a dedicated, specialized forum for all aspects of hardware research. It covers mainstream hardware security research, but also supports novel research and methods at an early stage, fostering innovation in the area. In this sense, the workshop also tries to support community building for the hardware security scene at

one of the largest computer security conferences in the world, ACM CCS.

2 WORKSHOP ORGANIZERS

The workshop had the following committees and chairs:

Steering Committee (SC): Chip Hong Chang (NTU Singapore, SC co-chair), Srini Devadas (MIT), Marten van Dijk (CWI and VU), Cetin Kaya Koc (UC Santa Barbara), Farinaz Koushanfar (UC San Diego), Debdeep Mukhopadhyay (IIT Kharagpur), Ulrich Rührmair (TU Berlin and U Connecticut, SC chair), Ahmad-Reza Sadeghi (TU Darmstadt), FX Standaert (UC Louvain), Mark Tehranipoor (U Florida), Ingrid Verbauwhede (KU Leuven)

Workshop Chairs: Chip Hong Chang (NTU Singapore), Ulrich Rührmair (TU Berlin and U Connecticut)

Program Committee Chairs: Lejla Batina (Radboud U), Domenic Forte (U Florida),

Program Committee: The full program committee had 64 members and is available from our webpage ashesworkshop.org.

Proceedings Chair: Francesco Regazzoni (U of Amsterdam and USI Lugano)

Publicity Chair: Naghmeh Karimi (UMBC)

Web Chair: Yuan Cao (Hohai University)

3 PREVIOUS WORKSHOP STATISTICS

The ASHES in 2017 in Dallas, Texas, USA, enjoyed 20 submissions and 37 participants. Geographically, submissions came mostly from institutions in the USA/Canada (10), followed by Europe (6), Asia (2), India (1) and Australia (1). 6 papers were eventually accepted, equaling an acceptance rate of 30%.

2018 in Toronto, Canada, ASHES collected 30 submissions, and 45 persons registered for the workshop. Geographically, submissions originated again mostly from authors associated with institutions in the USA and Canada (≈17), followed by Europe (≈12) and India (1). 10 submissions were eventually accepted, constituting a 33.3% acceptance rate.

2019 in London, UK, there were 36 submissions to the workshop, and 107 registered participants. Presumably due to the European location, 17 ASHES submissions came from Europe in that year, closely followed by the US & Canada (15), and Asia (3) and India (1). The workshop eventually hosted 11 accepted papers, amounting to a 30.6% acceptance rate.

2020 in Orlando, Florida, USA, there were 25 submissions. These originated from the USA (12), Europe (7), India (5), and Japan (1). The individual number of registered participants at ASHES was no longer available in this year, since CCS had changed the workshop registration process: Participants now registered for all pre-conference or post-conference workshops on the same day, not for a specific one. The workshop eventually featured 11 accepted papers, implying an acceptance rate of 44%.

2021 in Seoul, South Korea, there were 35 submissions, coming from the USA (18), Europe (9) and Asia (8). Again, the individual number of registered participants at ASHES was no longer available, since CCS had changed the workshop registration process (please compare above). The workshop eventually presented 11 accepted papers, translating to an acceptance rate of 31.4%.

2022 in Los Angeles, California, USA, there were 33 submissions, coming from the USA (16), Europe (13) and Asia (4). Again, the individual number of registered participants at ASHES was no longer available to us (please see above). The workshop eventually included 11 accepted papers, leading to a 33.3% acceptance rate.

2023 in Copenhagen, Denmark, there were 33 submissions. The workshop eventually included 12 accepted papers, leading to a 36.36% acceptance rate.

4 PROGRAM OF ASHES 2023

Our program hosted 12 technical papers distributed over 5 sessions. These were:

- Side-Channel Attacks
- Novel Attacks and Implementations
- Artificial Intelligence and Side-Channel Attacks
- Fault Attacks
- Reverse Engineering

In addition, 2 invited keynotes took place at the workshop. In alphabetical ordering:

- **Ravi Pappu (formerly MIT, now Apeiron Labs)**
  Physical Unclonable Functions: The First Fifty Years
- **Claire Vishik (former Intel Fellow and Group CTO, now co-founder and CTO of a stealth startup)**
  I*n Search of Trust: 30 Years of Evolution of Trusted Computing and Hardware Security*

The program, and any other information on the workshop, is available from the ASHES website under **ashesworkshop.org**.

ACKNOWLEDGEMENTS

UR received support by the EU-Project "NEUROPULS".