ASHES 2019 – CALL FOR PARTICIPATION

We are happy to announce the **Third Workshop on Attacks and Solutions in Hardware Security (ASHES 2019)**, taking place on **November 15, 2019 in London, UK**. ASHES is a post-conference satellite workshop of **ACM CCS 2019**, one of the premier computer security conferences.

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.

In this year, ASHES will host the following program:

INVITED KEYNOTE I

- F.-X. Standaert (UC Louvain): ***Towards an Open Approach for Side-Channel Resilient Authenticated Encryption***

SESSION NO. 1: PUFS AND PHYSICAL LAYER SECURITY

- Chongyan Gu (U Belfast) et al.: ***A Large Scale Comprehensive Evaluation of Single-Slice Ring Oscillator and PicoPUF Bit Cells on 28nm Xilinx FPGAs***
- Mitsuru Shiozaki (Ritsumeikan U) et al.: ***Simple Electromagnetic Analysis Attacks based on Geometric Leak on an ASIC Implementation of Ring-Oscillator PUF***
- Noriyuki Miura (Kobe U) et al.: ***A Replica-Based Light-Weight EM Immunity Test System for Secure and Safe FMCW Radar***

SESSION NO. 2: SIDE CHANNELS AND FAULT ATTACKS

- Aurélien Vasselle (eShard) et al.: ***Breaking Mobile Firmware Encryption through Near-Field Side-Channel Analysis***
- Keyvan Ramezanpour (Virginia Tech) et al.: ***Fault Intensity Map Analysis with Neural Network Key Distinguisher***
- Bodo Selmke (Fraunhofer AISEC) et al.: ***Peak Clock: Fault Injection into PLL-Based Systems via Clock Manipulation***

INVITED KEYNOTE II

- Ross Anderson (Cambridge University): ***Tamper Resistance 20 Years On***

SESSION NO. 3: REVERSE ENGINEERING AND TRUSTED MANUFACTURING

- Leonid Azriel (Technion) et al.: ***An Overview of Algorithmic Methods in IC Reverse Engineering***
- Yuqiao Zhang (Auburn) et al.: ***TGA: An Oracle-less and Topology-Guided Attack on Logic Locking***

SESSION NO. 4: FPGA-SECURITY AND MEMORY ATTACKS

- Sahan Bandara (Boston U) et al.: ***Adaptive Caches as a Defense Mechanism Against Cache Side-Channel Attacks***
- Florian Unterstein (Fraunhofer AISEC) et al.: ***SCA Secure and Updatable Crypto Engines for FPGA SoC Bitstream Decryption***
- Mathieu Gross (TU Munich) et al.: ***Breaking TrustZone memory isolation through Malicious Hardware on a modern FPGA-SoC***

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, Founder)
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)

Publication Chair

Francesco Regazzoni (U Lugano)

Web Chair

Yuan Cao (Hohai U)

Invited Keynotes

Ross Anderson,
Cambridge University:

Tamper Resistance 20 Years On

Francois-Xavier Standaert,
UC Louvain

Towards an Open Approach for Side-Channel Resilient Authenticated Encryption

ashesworkshop.org