2017 Asian Hardware Oriented Security and Trust Symposium (AsianHOST 2017)

Beijing, China
19 – 20 October 2017
Technical Program

AsianHOST 2017 Program Highlights

- 6 Featured Invited Speakers showcasing some of the world’s leading innovative thinkers in hardware security! It includes 2 Keynote Talks and 4 Visionary Talks.
- 22 Technical Papers
- One panel on industrial view towards hardware security in Asia
- Cisco Best Paper Award

Thursday, October 19, 2017

7:15 - 8:15AM  Registration

SESSION 1: PLENARY SESSION
Moderator: Gang Qu, University of Maryland

8:15 - 8:30AM  Opening Remarks: AsianHOST 2017 General and Program Chairs

8:30 - 8:45AM  Welcome Remarks
Speaker: Zheng You, Vice President of Tsinghua University, Member of China Engineering Academy
Title: Hardware Security in Asia.....N/A

8:45 - 9:30AM  KEYNOTE I
Speaker: Shaojun Wei, Tsinghua University
Title: Reconfigurable Computing and Hardware Security.....N/A

9:30 - 10:00AM  VISIONARY TALK
Speaker: Ramesh Karri, New York University
Title: Towards Securing Biochips.....N/A

10:00 - 10:30AM  BREAK
10:30 - 11:50AM  SESSION 2: IP/IC PROTECTION
Session Chair: Pingqiang Zhou, ShanghaiTech University

• *DOST: Dynamically Obfuscated Wrapper for Split Test against IC Piracy.....1
  Xiaoxiao Wang, Yueyu Guo, and Dongrong Zhang - Beihang University
  M. Tauhidur Rahman, and Mark Tehranipoor - U. of Florida

• PCH Framework for IP Runtime Security Verification.....79
  Xiaolong Guo, Jiaji He, and Yier Jin - University of Florida
  Raj Gautam Dutta - University of Central Florida

• Secure Integration of Non-Truste d IPs in SoCs.....103
  Festus Hategekimana, Taylor Whitaker, Md Jubaer Hossain and Christophe Bobda -
  University of Arkansas

• Scalable Security Path Methodology: A Cost-security Trade-off to Protect FPGA IPs
  against Active and Passive Tampers.....85
  Sharareh Zamanzadeh and Ali Jahanian - Shahid Beheshti University

*Cisco Best Paper Candidate

11:50 - 1:20PM   LUNCH

1:20 - 1:50PM  SESSION 3: VISIONARY TALK
Session Chair: Jing Ye, Chinese Academy of Science
Speakers: Swarup Bhunia and Domenic Forte, U. of Florida
Title: Security of the Internet of Things: New Frontiers.....N/A

1:50 - 3:30PM  SESSION 4: PHYSICAL UNClONABLE FUNCTION AND RANDOM NUMBER GENERATOR
Session Chair: Jiun-Lang Huang, National Taiwan University

• *On-chip Jitter Measurement for True Random Number Generators.....91
  Bohan Yang, Vladimir Rozic, Milos Grujic, Nele Mentens and Ingrid Verbauwhede -
  IMEC-COSIC, KU Leuven

2017 Asian Hardware Oriented Security and Trust Symposium (AsianHOST 2017)
• *An Energy-efficient True Random Number Generator Based on Current Starved Ring Oscillators.....37
  Yuan Cao, Chip Hong Chang, and Yue Zheng - Nanyang Technological University
  Xiaojin Zhao - Shenzhen University

• Implementation of Stable PUFs Using Gate Oxide Breakdown.....13
  Wei-Che Wang, Yair Yona, Yizhang Wu, Szu-Y ao Hung, Suhas Diggavi, and Puneet Gupta - UCLA

• The Impact of Discharge Inversion Effect on Learning SRAM Power-Up Statistics.....31
  Zhonghao Liao, George A mariucai, Raymond Wong and Yong Guan - Iowa State U.

• Polymorphic PUF: Exploiting Reconfigurability of CPU+FPGA SoC to Resist Modeling Attack.....43
  Jing Ye, Yue Gong, Yu Hu and Xiaowei Li - Institute of Computing Technology,
  Chinese Academy of Sciences

*Cisco Best Paper Candidate

3:30 - 3:50PM    BREAK

3:50 - 5:30PM    SESSION 5: IOT AND CPS SECURITY

Session Chair: Wei Sheng, University of Nebraska-Lincoln

• Secure Intra-Vehicular Communication over CANFD.....97
  Ali Shuja Siddiqui, Chia-Che Lee, and Fareena Saqib - University of North Carolina at Charlotte
  Wenjie Che and Jim Plusquellic - University of New Mexico

• Mixed-Granular Architectural Diversity for Device Security in the Internet of Things.....73
  Robert Karam, Tamzidul Hoque, Kevin Butler and Swarup Bhunia - U. of Florida

• Obfuscating Branch Decisions based on Encrypted Data using MISR and Hash Digests.....115
  Nektarios Georgios Tsoutsos - New York University
  Michail Maniatakos - New York University Abu Dhabi

2017 Asian Hardware Oriented Security and Trust Symposium (AsianHOST 2017)
• **MPA: Model-assisted PCB Attestation via Board-level RO and Temperature Compensation** ..... 25
  Zimu Guo, Xiaolin Xu, Mark Tehranipoor and Domenic Forte - University of Florida

• **'The Dangers of Sleeping', an Exploration of Security in Non-Volatile Processors** ..... 121
  Patrick Cronin and Chengmo Yang - University of Delaware
  Dongqin Zhou and Keni Qui - Capital Normal University
  Xin Shi and Yongpan Liu - Tsinghua University

6:30 - 8:30PM **DINNER AND AWARD CEREMONY**

**Ceremony Moderator:**
  Huaquiang Wu, Deputy Director, Beijing Innovation Center for Future Chip, Tsinghua University

**Cisco Best Paper Award Presenter:**
  Yousef Iskandar, Cisco

---

**Friday, October 20, 2017**

7:30 - 8:30AM **Registration**

**SESSION 6: PLENARY SESSION**

**Moderator:** Yier Jin, University of Florida

8:30 - 9:15AM **KEYNOTE II**

**Speaker:** Marilyn Claire Wolf, Georgia Tech

**Title:** Hardware-oriented Security, CPS and IoT.....N/A

9:15 - 9:50AM **VISIONARY TALK**

**Speaker:** Wenyuan Xu, Zhejiang University and University of South Carolina

**Title:** Analog Security of Cyber-Physical Systems - From 0101 to Mixed Signals.....N/A

9:50 - 10:20AM **BREAK**
10:20 - 11:40AM  **SESSION 7: SIDE-CHANNEL ANALYSIS AND PHYSICAL UNCLONABLE FUNCTION**  
**Session Chair:** Xiaoxiao Wang, Beihang University

- **Improved low-entropy masking scheme for LED with mitigation against correlation-enhanced collision attacks...** 49  
  Fan Zhang, Liang Geng, and Jizhong Shen - Zhejiang University  
  Shivam Bhasin - Nanyang Technological University  
  Xinjie Zhao and Shize Guo - The Institute of North Electronic Equipment

- **A New Key Rank Estimation Method to Investigate Dependent Key Lists of Side Channel Attacks...** 19  
  Shuang Wang, Yang Li and Jian Wang - Nanjing University of Aeronautics and Astronautics

- **Extending 1kb RRAM Array from Weak PUF to Strong PUF by Employment of SHA Module...** 67  
  Rui Liu and Shimeng Yu - Arizona State University  
  Huaqiang Wu, Yachuan Pang, and He Qian - Tsinghua University

- **PUFSec: Protecting Physical Unclonable Functions Using Hardware Isolation-based System Security Techniques...** 7  
  Mengmei Ye, Mehrdad Zaker Shahrak, and Sheng Wei - University of Nebraska-Lincoln

12:00 - 1:00PM  **Lunch**

1:00 - 1:30PM  **SESSION 8: VISIONARY TALK**  
**Session Chair:** Domenic Forte, University of Florida  
**Speaker:** Yousef Iskander, CISCO  
**Title:** Making Hardware Security and Trust the Next Market Differentiator...N/A

1:30 - 2:50PM  **SESSION 9: ATTACKS AND DEFENSES**  
**Session Chair:** Chengmo Yang, University of Delaware

- **A Split Manufacturing Approach for Unclonable Chipless RFIDs for Pharmaceutical Supply Chain Security...** 61  
  Kun Yang, Ulbert Botero, Haoting Shen, Domenic Forte and Mark Tehranipoor - University of Florida

2017 Asian Hardware Oriented Security and Trust Symposium (AsianHOST 2017)
• **A Practical Cold Boot Attack on RSA Private Keys....55**
  Tian Wang, Xiaoxin Cui, Yewen Ni, and Dunshan Yu - Peking University
  Xiaole Cui - Peking University Shenzhen Graduate School
  Gang Qu - University of Maryland

• **Employing Dual-complementary Flip-Flops to Detect EMFI Attacks....109**
  Chinmay Deshpande, Bilgiday Yuce, Patrick Schaumont and Leyla Nazhandali - Virginia Tech

• **Evaluating Obfuscation Performance of Novel Algorithm-to-Architecture Mapping Techniques in Systolic-Array-based Circuits....127**
  Jiafeng Xie - Wright State University
  Xiaojun Zhou - Central South University

2:50 – 3:50PM **SESSION 10: PANEL**
**Topic:** Global Electronic Supply Chain Security: What Can Asian Pacific Region Do About it?
**Panel Organizers:** Yousef Iskander and Mark Tehranipoor
**Panel Moderator:** Yousef Iskander, Cisco
**Panelists:**
  - Mark Tehranipoor - University of Florida
  - Xiaowei Li - Institute of Computing Technology Chinese Academy of Science (ICT)
  - Brian Cohen - Institute for Defense Analyses (IDA)
  - Qiang Xu - Chinese University of Hong Kong
  - Gang Qu - University of Maryland

3:50 - 4:00PM **Closing Remarks**