HOST 2015 Program
May 5-7, 2015
McLean, VA, USA
The Ritz-Carlton, Tysons Corner

Tuesday, May 5

8:45 - 9:00 Opening Remarks
HOST 2015 General and Program Chairs

9:00 - 10:00 SESSION 1: KEYNOTE I
Session Chair: Mark Tehranipoor, U. of Connecticut

Keynote talk: IOT Security: Challenges and Solutions
By Dr. RAMESH SEPEHRRAD
Vice President, National Governance, Risk and Compliance
Comcast

10:00 - 10:20 BREAK

10:20 - 11:35 SESSION 2: INVITED INDUSTRIAL SESSION
Session Chair: Mark Tehranipoor, U. of Connecticut
2. Jim Fahrny, Senior Fellow, Comcast Comcast’s view of Security
3. Ken Heffner, Fellow, Honeywell Honeywell’s view of Security

11:45 - 1:00 LUNCH

Plenary Talk:
12:10 – 12:30 Microsemi

1:00 - 2:15 SESSION 3: EFFICIENT IMPLEMENTATION OF SECURE SYSTEMS
Session Chair: Qiaoyan Yu, University of New Hampshire
• Aria Shahverdi, Mostafa Taha and Thomas Eisenbarth. Silent SIMON: A Threshold Implementation under 100 Slices
• Mudit Bhargava, Kaship Sheikh and Ken Mai. Robust True Random Number Generator Using Hot-Carrier Injection Balanced Metastable Sense Amplifiers
- Kan Xiao, Domenic Forte and Mohammad Tehranipoor. Efficient and Secure Split Manufacturing via Obfuscated Built-In Self-Authentication

2:15 - 2:35 BREAK

2:35 - 3:50 SESSION 4: PUF
Session Chair: Ioannis Savidis, Drexel University

- Georg T. Becker, Alexander Wild and Tim Güneysu. Security Analysis of Index-Based Syndrome Coding for PUF-Based Key Generation
- Pai-Yu Chen, Runchen Fang, Rui Liu, Chaitali Chakrabarti, Yu Cao and Shimeng Yu. Exploiting Resistive Cross-point Array for Compact Design of Physical Unclonable Function
- Cheng-Wei Lin and Swaroop Ghosh. A Family of Schmitt-Trigger-based Arbiter-PUFs and Selective Challenge-Pruning for Robustness and Quality

4:00 - 5:50 SESSION 5: POSTER SESSION
Session Chair: Garrett S. Rose, University of Tennessee

See below for the list of poster presentations

6:00 RECEPTION

---

**Wednesday, May 6**

9:00 - 10:00 SESSION 6: KEYNOTE II
Session Chair: Saverio Fazzari, Booz Allen Hamilton

**Keynote talk:** *Is it safe?*
By **Mr. W. ERIC HERR**
Director, Technology Integration Office (TIO)
Office of the Under Secretary of Defense (AT&L)

10:00 - 10:15 BREAK

10:15 - 11:45 SESSION 7: PANEL
"What are People looking for from Hardware Security Research?"
Moderators: Saverio Fazzari, Booz Allen Hamilton & Mark Tehranipoor, U. of Connecticut
1. Kerry Bernstein, DARPA
2. Serge Leef, Mentor Graphics
3. TBA, Northrup Grumman
4. Nina Amla, NSF
5. Celia Merzbacher, SRC

11:45 - 1:00 LUNCH

Plenary Talk:
12:10 – 12:30 Honeywell

1:00 - 2:15 SESSION 8: INVITED GOVERNMENT SESSION
Session Chair: Saverio Fazzari, Booz Allen Hamilton
1. Arnett Brown, Booz Allen Hamilton DARPA SHIELD Program
2. Matt Casto, AFRL, Dayton OH AFRL Trusted Initiative
3. Brett Hamilton, NAVSEA-CRANE OSD Harward Assurance Initiative

2:15 – 2:30 BREAK

2:30 - 3:45 SESSION 9: SIDE CHANNEL AND FAULT ATTACKS ANALYSIS I
Session Chair: Yier Jin, U. of Central Florida
- Dhiman Saha and Dipanwita Roy Chowdhury. Diagonal Fault Analysis of Grøstl in Dedicated MAC Mode
- Richard Gilmore, Neil Hanley and Maire O'Neill. Neural Network Based Attack on a Masked Implementation of AES
- Nail Etkin Can Akkaya, Burak Erbagci, Raymond Carley and Ken Mai. A DPA-Resistant Self-Timed Three-Phase Dual-Rail Pre-Charge Logic Family

3:45 – 4:00 BREAK

4:00 – 5:15 SESSION 10: SIDE CHANNEL AND FAULT ATTACKS ANALYSIS II
Session Chair: Domenic Forte, U. of Connecticut
- Liwei Zhang, A. Adam Ding, Yunsi Fei and Pei Luo. Efficient 2nd-order Power Analysis on Masked Devices Utilizing Multiple Leakage
- Xiaofei Guo, Nagmeh Karimi, Francesco Regazzoni, Chenglu Jin and Ramesh Karri. Simulation and Analysis of Negative-Bias Temperature Instability Aging on Power Analysis Attacks
- Pascal Sasdrich, Amir Moradi, Oliver Mischke and Tim Güneysu. Achieving Side-Channel Protection with Dynamic Logic Reconfiguration on Modern FPGAs
Thursday, May 7

9:00 - 10:00 SESSION 11: KEYNOTE III
Session Chair: James Plusquellic, University of New Mexico

Keynote talk: SoC Security Objectives: What Does Your Market Say?
By Dr. DHINESH MANOHARAN
Director, Product Security Research, Security Center of Excellence
Intel

10:00 - 10:20 BREAK

10:20 - 11:35 SESSION 12: HARDWARE TROJAN HORSES, SECURITY ANALYSIS, EVALUATIONS, AND METRICS
Session Chair: Houman Homayoun, George Mason University
- Pramod Subramanyan, Sayak Ray and Sharad Malik. Evaluating the Security of Logic Encryption Algorithms
- Ian Wilcox, Fareena Saqib and Jim Plusquellic. GDS-II Trojan Detection using Multiple Supply Pad VDD and GND IDDQs in ASIC Functional Units
- Ingrid Exurville, Zussa Loïc, Jean-Baptiste Rigaud and Bruno Robisson. Resilient Hardware Trojans Detection based on Path Delay Measurements

11:35 - 12:25 SESSION 13: SECURE AND TRUSTED SYNTHESIS AND DESIGN
Session Chair: Gregory L. Creech, ElectroScience Laboratory, Ohio State University
- Roarke Horstmeyer, Sid Assawaworrarit, Ulrich Ruhrmair and Changhuei Yang. Physically secure and fully reconfigurable data storage using optical scattering

12:30 CONCLUDING REMARKS
HOST 2015 Program Chairs

Posters:
- Meng-Day (Mandel) Yu, Matthias Hiller and Srinivas Devadas. Maximum Likelihood Decoding of Device-Specific Multi-Bit Symbols for Reliable Key Generation
- Abhishek Chakraborty, Bodhisatwa Mazumdar and Debdeep Mukhopadhyay. A Practical DPA on Grain v1 using LS-SVM
- Gedare Bloom, Bhagirath Narahari, Rahul Simha, Ali Namazi and Renato Levy. FPGA SoC Architecture and Runtime to Prevent Hardware Trojans from Leaking Secrets
- Chongxi Bao, Yang Xie and Ankur Srivastava. A Security-aware Design Scheme for Better Hardware Trojan Detection Sensitivity
- Carlos Tadeo Ortega Otero, Jonathan Tse, Robert Karmazin, Benjamin Hill and Rajit Manohar. Automatic Obfuscated Cell Layout for Trusted Split-Foundry Design
- Lionel Rivièrè, Zakaria Najm, Pablo Rauzy, Jean-Luc Danger, Julien Bringer and Laurent Sauvage. High Precision Fault Attacks on the Instruction Cache of ARMv7-M Architectures
- Zachary N. Goddard, Nicholas Lajeunesse and Thomas Eisenbarth. Power Analysis of the t-Private Logic Style for FPGAs
- Bilgiday Yuce, Nahid Farhady Ghalaty and Patrick Schaumont. TVVF: Estimating the Vulnerability of Hardware Cryptosystems against Timing Violation Attacks
- Athanasios Papadimitriou, Marios Tampas, David Hély, Vincent Beroulle, Paolo Maistri and Regis Leveugle. Validation of RTL Laser Fault Injection Model with respect to Layout Information
- Xuan Thuy Ngo, Sylvain Guilley, Shivam Bhasin, Zakaria Najm and Jean-Luc Danger. Linear Complementary Dual Code Improvement to Strengthen Encoded Circuit Against Hardware Trojan Horses
- Shamit Ghosh and Dipanwita Roy Chowdhury. Preventing Fault Attack on Stream Cipher using Randomization
- Qian Wang, An Wang, Liji Wu and Gang Qu. Template Attack on Masking AES Based on Fault Sensitivity Analysis