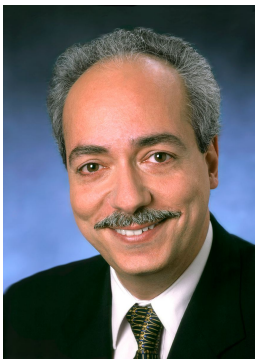
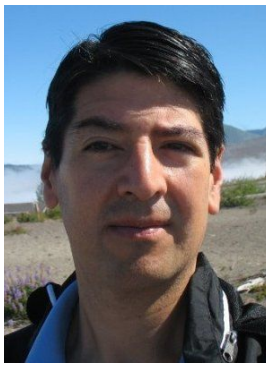
Featured Speakers

KEYNOTE
Paul Kocher
Cryptography Research



VISIONARY TALK
Yervant Zorian
Synopsys



VISIONARY TALK
Carlos V. Rozas
Intel

KEYNOTE
Jeremy Muldavin
OSD

VISIONARY TALK
Ahmad-Reza Sadeghi
Tech. Universität Darmstadt

KEYNOTE
Todd Austin
U. of Michigan

KEYNOTE
Cliff Wang
ARO

Monday (Tutorial Day), May 1 | Salon I 5th floor & Old Dominion Room, 4th Floor

1:00 – 3:30pm TUTORIAL 1 and TUTORIAL 2

Tutorial Chair: Domenic Forte, U. of Florida

T1*. Protecting Electronics Supply Chain from Design to Resign*
Prof. Mark Tehranipoor, University of Florida
Location: Salon I, 5th Floor

T2. *Trusted Platform Modules and Their Applicability to Hardware and Software Security Mitigations*
Topher Timzen, Intel Security Center of Excellence (SeCoE)
Chandni Bhowmik, Intel Security Center of Excellence (SeCoE)
Location: Old Dominion Room, 4th Floor

3:30 – 4:00pm Afternoon Break - Refreshments available at Old Dominion Room

4:00 – 6:30pm TUTORIAL 3 and TUTORIAL 4

T3. *Security and Trust in the Analog/Mixed-Signal/RF Domain: A Survey and a Perspective*
Prof. Yiorgos Makris, The University of Texas at Dallas
Location: Old Dominion Room, 4th Floor

T4. *Hardware Security and Trust Challenges in Emerging IoT Systems and Applications*
Prof. Fareena Saqib, Florida Institute of Technology
Prof. Jim Plusquellic, University of New Mexico
Prof. Mohammad Al Faruque, University of California-Irvine
Location: Salon I, 5th Floor

Tuesday, May 2 | Salon 2 & 3, 5th Floor

7:30 – 8:30am Registration and Continental Breakfast

8:30 – 8:45am Opening Remarks

Speaker: HOST 2017 General and Program Chairs

8:45 – 9:00am HOST 10th Anniversary Ceremony

9:00 – 9:45am KEYNOTE

Speaker: Paul Kocher, Cryptography Research, Inc. / Rambus
Title: *Improbabilities of Security*

9:45 – 10:15am INVITED VISIONARY TALK

Speaker: Yervant Zorian, Synopsys Chief Architect and Fellow
Title: *The Role of Infrastructure IP in Securing SOCs*

10:15 – 11:00am HARDWARE DEMO COMPETITION & POSTERS

11:00 – 12:20pm REGULAR PAPER SESSION 1: Architecture Level Security
Session Chair: Aaron Cohen, US Naval Research Laboratory

- *Intrinsic Rowhammer PUFs: Leveraging the Rowhammer Effect for Improved Security*
  André Schaller, Muhammad Umair Saleem, Nikolaos A. Anagnostopoulos, Stefan Katzenbeisser - *Technische Universität Darmstadt, Germany*
  Wenjie Xiong, Jakub Szefer - *Yale University, USA*
- *When Good Protections Go Bad: Exploiting Anti-DoS Measures to Accelerate Rowhammer Attacks*
  Misiker Tadesse Aga, Zelalem Birhanu Aweke and Todd Austin - *University of Michigan, USA*
- *Secure Heterogeneous Multicore Architecture Design*
  Michel Kinsy, Shreeya Khadka, Mihailo Isakov and Anam Farrukh - *Boston University, USA*
- *Reviving Instruction Set Randomization*
  Kanad Sinha, Simha Sethumadhavan - *Columbia University, USA*
  Vasilis Kemerlis - *Brown University, USA*

12:20 – 1:30pm LUNCH

12:30 – 12:50pm LUNCH TALK

Speaker: Jim Plusquellic, CTO, Enthentica; Professor, University of New Mexico
Title: *Hardware-Based Security and Trust For IoT and Supply Chain Authentication*

1:30 – 3:00pm REGULAR PAPER SESSION 2: Primitives and Implementations
Session Chair: Wayne A. Reed, KCNSC

- *Creating Security Primitive by Nanoscale Manipulation*
  Zhaoying Hu - *State University of New York at Albany, USA*
  Shu-Jen Han - *IBM Research, USA*
- *Automatic Generation of High-Performance Modular Multipliers for Arbitrary Mersenne Primes on FPGAs*
  Philipp Koppermann, Johann Heyszl - *Fraunhofer AISEC, Germany*
  Fabrizio De Santis, Georg Sigl - *Technische Universität München, Germany*
- *Efficient Configurations for Block Ciphers with Unified ENC/DEC Paths*
  Subhadeep Banik - *Temasek LABS, Singapore*
  Andrey Bogdanov - *Technical University of Denmark, Denmark*
  Francesco Regazzoni - *ALaRI - USI, Switzerland*

- *Memory-Constrained Implementation of Lattice-based Encryption Scheme on Standard Java Card*
  Ye Yuan, Tsuyoshi Takagi - *Kyushu University, Japan*
  Kazuhide Fukushima, Shinsaku Kiyomoto - *KDDI Research, Inc., Japan*
- *Towards a Memristive Hardware Secure Hash Function (MemHash)*
  Leonid Azriel and Shahar Kvatinsky - *Technion - Israel Institute of Technology, Israel*

3:00 – 4:00pm HARDWARE DEMO COMPETITION & POSTERS

4:00 – 4:30pm KEYNOTE

Speaker: Todd M. Austin, Univ. of Michigan
Title: *Establishing Hardware Trust: Challenges, Opportunities and (Im)possibilities*

4:30 – 5:45pm PANEL I: DoD and Hardware Security

Moderator: Saverio Fazzari, Booz Allen

Panelists:
Matthew Casto, Air Force Research Lab
Jeremy Muldavin, OSD
Brett Hamilton, Navy
Christine Rink, The Aerospace Corporation

Wednesday, May 3 | Salon 2 & 3, 5th Floor

7:45 – 8:45am Registration and Continental Breakfast

8:45 – 9:30am KEYNOTE

Speaker: Jeremy Muldavin, OSD
Title: *Long-Term Strategy for DoD Trusted and Assured Microelectronics Needs*

9:30 – 10:00am INVITED VISIONARY TALK

Speaker: Ahmad-Reza Sadeghi, Technische Universität Darmstadt, Germany
Title: *Hardware-assisted Security: So Close yet So Far*

10:00 – 11:05am: HARDWARE DEMO COMPETITION & POSTERS

11:05 – 12:20pm REGULAR PAPER SESSION 3: Side-Channel Attack/Analysis

Session Chair: Alpa Trivedi, Intel

- *Stateless Leakage Resiliency from NLFSRs*
  Mostafa Taha, Arash Reyhani-Masoleh - *Western University, Canada*
  Patrick Schaumont - *Virginia Tech, USA*
- *High Efficiency Power Side-Channel Attack Immunity using Noise Injection in Attenuated Signature Domain*
  Debayan Das, Shovan Maity, Shreyas Sen - *Purdue University, USA*
  Saad Bin Nasir, Arijit Raychowdhury - *Georgia Institute of Technology, USA*

Santosh Ghosh - *Intel Labs, USA*

- *Exploring Timing Side-channel Attacks on Path-ORAMs*
  Chongxi Bao and Ankur Srivastava - *University of Maryland, College Park, USA*
- *Photonic Side Channel Attacks Against RSA*
  Elad Carmon - *Tel Aviv University, Israel*
  Jean-Pierre Seifert and - *Deutsche Telekom AG, Germany*
  Avishai Wool - *Tel Aviv University, Israel*

12:20 – 1:30pm LUNCH

12:30 – 12:50pm LUNCH TALK

Speaker: Pim Tuyls, CEO, Intrinsic-ID
Title: *IoT: Heaven or Hell*

1:30 – 2:50pm REGULAR PAPER SESSION 4: New Attacks

Session Chair: Fareena Saqib, Florida Institute of Technology

- *Characterising a CPU Fault Attack Model via Run-Time Data Analysis*
  Martin Kelly, Keith Mayes - *Royal Holloway, University of London, United Kingdom*
  John Walker - *DNV GL Ltd., United Kingdom*
- *Breaking Active-Set Backward-Edge CFI*
  Michael Theodorides and David Wagner - *University of California, Berkeley, USA*
- *INFECT: INcospicuous FEC-based Trojan: a Hardware Attack on an 802.11a/g Wireless Network*
  Kiruba S. Subramani, Angelos Antonopoulos, Ahmed Abotabl, Aria Nosratinia and Yiorgos Makris - *University of Texas at Dallas, USA*
- *A Novel Physiological Features-Assisted Architecture for Rapidly Distinguishing Health Problems from Hardware Trojan Attacks and Errors in Medical Devices*
  Taimour Wehbe, Vincent J. Mooney, Abdul Qadir Javaid and Omer T. Inan - *Georgia Institute of Technology, USA*
- *Challenging On-Chip SRAM Security with Boot-State Statistics*
  Joseph McMahan, Weilong Cui, Liang Xia, Timothy Sherwood - *University of California, Santa Barbara, USA*
  Jeff Heckey - *Avago Technologies, USA*
  Frederic T. Chong - *University of Chicago, USA*

2:50 – 4:00pm POSTERS & HARDWARE DEMO

4:00 – 5:30pm PANEL II: Security and Architecture

Moderator: Julien Carreño, Security Architecture Lead, Intel

Panelists:
Milos Prvulovic, Georgia Tech
Yan Solihin, NC State University
Sandip Ray, NXP Semiconductor
Serge Leef, Mentor Graphics

Yousef Iskander, Cisco

6:00pm RECEPTION and AWARD ANNOUNCEMENTS

Thursday, May 4 | Salon 2 & 3, 5th Floor

7:45 – 8:45am Continental Breakfast

8:45 – 9:30am KEYNOTE

Speaker: Cliff Wang, Army Research Office
Title: *Cyber deception: An emerging cyber security research thrust*

9:30 – 10:00am INVITED VISIONARY TALK

Speaker: Carlos V. Rozas, Intel, Portland, USA
Title: *Hardware based Security and the Cloud*

10:00 – 10:20am BREAK

10:20 – 12:00pm REGULAR PAPER SESSION 5: Enhanced HW Security
Session Chair: Greg Creech, GLC Consulting

- *AppSAT: Approximately Deobfuscating Integrated Circuits*
  Kaveh Shamsi, Travis Meade, Yier Jin - *University of Central Florida, USA*
  Meng Li, Zheng Zhao, David Z. Pan - *University of Texas at Austin, USA*
- *Using Computational Game Theory To Guide Verification and Security in Hardware Designs*
  Andrew M. Smith - *Sandia National Laboratories & University of California, Davis, USA*
  Jackson Mayo, Vivian Kammler, Robert C. Armstrong - *Sandia National Laboratories, USA*
  Yevgeniy Vorobeychik - *Vanderbilt University, USA*
- *Physical Unclonable Functions and Dynamic Partial Reconfiguration for Security in Resource-Constrained Embedded Systems*
  Goutham Pocklassery, Venkata Kishore Kajuruli, Fareena Saqib and Jim Plusquellic - *University of New Mexico, USA*
- *New Clone-Detection Approach for RFID-Based Supply Chains*
  Hoda Maleki, Reza Rahaeimehr, Chenglu Jin and Marten van Dijk
  - University of Connecticut, USA
- *Take a Moment and have some t: Hypothesis Testing on Raw PUF Data*
  Vincent Immler, Matthias Hiller, Johannes Obermaier - *Fraunhofer AISEC, Germany*
  Georg Sigl - *Technische Universität München, Germany*

12:00 – 1:00pm LUNCH

12:10 – 12:30pm LUNCH TALK

Speaker: Jason Sanabia, CTO, President & CEO, Raith America

Title: *Latest Developments in Large Area, High Resolution SEM and FIB for Semiconductor Reverse Engineering*

1:00 – 2:00pm REGULAR PAPER SESSION 6: Physical Unclonable Functions

Session Chair: Sanghamitra Roy, Utah State University

- *A New Maskless Debiasing Method for Lightweight Physical Unclonable Functions*
  Aydin Aysu, Ye Wang, Michael Orshansky - *University of Texas Austin, USA*
  Patrick Schaumont - *Virginia Tech, USA*
- *A Stochastic All-Digital Weak Physically Unclonable Function for Analog/Mixed-Signal Applications*
  Troy Bryant, Sreeja Chowdhury, Domenic Forte, Mark Tehranipoor and Nima Maghari - *University of Florida, USA*
- *Improving Reliability of Weak PUFs via Circuit Techniques to Enhance Mismatch*
  Vinay C Patil, Arunkumar Vijayakumar, Daniel E. Holcomb and Sandip Kundu - *University of Massachusetts Amherst, USA*

2:00 pm CONCLUDING REMARKS

Speakers: HOST 2017 and HOST 2018 General and Program Chairs

CO-LOCATED WORKSHOPS

Thursday, May 4, 2:30 – 6:00pm | Salon 2, 5th Floor

The 1st Workshop for Women in Hardware Systems Security (WISE)

Friday, May 5, 8:30 am – 1:30pm | Old Dominion Hall, 4th Floor

Internet of Things (IoT) and Automotive Security Workshop (IASW)

POSTERS:

Poster Session Chair: Wujie Wen, Florida International University

- *Ag Conductive Bridge RAMs for Physical Unclonable Functions*
  Bertrand Cambou, Fatemeh Afghah, Derek Sonderegger - *Northern Arizona University, USA*
  Jennifer Taggart, Hugh Barnaby and Michael Kozicki - *Arizona State University, USA*
- *Fabrication Security and Trust of Domain-Specific ASIC Processors*
  Michael Vai, Karen Gettings and Theodore Lyszczarz - *MIT Lincoln Laboratory, USA*
- *Øzone: Efficient Execution with Zero Timing Leakage for Modern Microarchitectures*
  Zelalem Birhanu Aweke and Todd Austin - *University of Michigan, USA*
- *LWE-Based Lossless Computational Fuzzy Extractor for the IoT*
  Christopher Huth, Paul Duplys - *Robert Bosch GmbH, Germany*
  Daniela Becker, Jorge Guajardo - *Robert Bosch LLC, USA*
  Tim Günesyu - *University of Bremen & DFKI*
- *Cache Timing Attacks on Recent Microarchitectures*
  Alexandros Andreou, Andrey Bogdanov and Elmar Tischhauser - *Technical University of Denmark, Denmark*
- *Analyzing Security Vulnerabilities of Three-Dimensional Integrated Circuits*
  Jaya Dofe and Qiaoyan Yu - *University of New Hampshire, USA*
- *A Novel Offset Method for Improving Bitstring Quality of a Hardware-Embedded Delay PUF*
  Wenjie Che, Jim Plusquellic- *University of New Mexico, USA*
  Fareena Saqib - *Florida Institute of Technology, USA*
- *Malicious CAN-message Attack against Advanced Driving Assistant System*
  Mitsuru Shiozaki, Masashi Nakano, Yuuki Nakazawa, Takaya Kubota and Takeshi Fujino - *Ritsumeikan University, Japan*
- *Improving FPGA based SHA-3 structures*
  Magnus Sundal and Ricardo Chaves - *IST / INESC-ID, Portugal*
- *On Secure Implementations of Quantum-Resistant Supersingular Isogeny Diffie-Hellman*
  Brian Koziel - *Texas Instruments, USA*
  Reza Azarderakhsh - *Florida Atlantic University, USA*
  David Jao - *University of Waterloo, USA*
- *Protecting Analog Circuits with Parameter Biasing Obfuscation*
  Vaibhav Venugopal Rao and Ioannis Savidis - *Drexel University, USA*
- *Circuit Recognition with Deep Learning*
  Yu-Yun Dai and Robert Brayton - *University of California, Berkeley, USA*
- *Detection of Counterfeit ICs using Public Identification Sequences*
  Peter Samarin and Kerstin Lemke-Rust - *Bonn-Rhein-Sieg, University of Applied Sciences, Germany*
- *Threshold Voltage Defined Multi-Input Complex Gates*
  Asmit De and Swaroop Ghosh - *Pennsylvania State University, USA*
- *Platform Agnostic, Scalable, and Unobtrusive FPGA Gateway Implementation of Moving Target Defense over IPv6 (MT6D)*
  Joseph Sagisi, Joe Tront and Randy Marchany - *Virginia Tech, USA*
- *TTLock: Tenacious and Traceless Logic Locking*
  Muhammad Yasin - *New York University, USA*
  Bodhisatwa Mazumdar - *Indian Institute of Technology Indore, India*
  Jeyavijayan Rajendran - *University of Texas at Dallas, USA*
  Ozgur Sinanoglu - *New York University Abu Dhabi, USA*

- *Exploiting Safe Error Based Leakage of RFID Authentication Protocol using Hardware Trojan Horse*
  Krishna Bagadia, Urbi Chatterjee, Debapriya Basu Roy, Debdeep Mukhopadhyay and Rajat Subhra Chakraborty - *Indian Institute of Technology Kharagpur, India*
- *Characterizing EEPROM for usage as a ubiquitous PUF source*
  Christopher Pavlina - *Binghamton University, USA*
  Jacob Torrey, Kyle J. Temkin - *Assured Information Security, USA*
- *On Designing Optimal Camouflaged Layouts*
  Thomas Broadfoot, Carl Sechen and Jeyavijayan Rajendran - *University of Texas at Dallas, USA*
- *Connecting the Dots: Privacy Leakage via Write-Access Patterns to the Main Memory*
  Tara John, Syed Kamran Haider, Hamza Omar and Marten van Dijk - *University of Connecticut, USA*
- *Correlation Power Analysis Attack against STT-MRAM Based Cyptosystems*
  Abhishek Chakraborty, Ankit Mondal and Ankur Srivastava - *University of Maryland, College Park, USA*
- *Synthesis of Hardware Sandboxes for Trojan Mitigation in Systems on Chip*
  Christophe Bobda, Taylor Whitaker - *University of Arkansas, USA*
  Charles Kamhoua, Kevin Kwiat, Laurent Njilla - *Air Force Research Laboratory, USA*

HARDWARE DEMOS:

Hardware Demo Chair: Jim Plusquellic, University of New Mexico

- *Supply Chain and IoT PUF-based Authentication* W. Che, G. Pocklassery, V. Kajuluri, F. Saqib and J. Plusquellic - *Florida Institute of Technology and U. of New Mexico*
- *Why Do You Trust Sensors? Analog Cybersecurity Attack Demos* A. Kwong, C. Bolton, T. Trippel, W. Xu and K. Fu - *U. of Michigan*
- *Complete Activation Scheme for IP Design Protection* B. Colombier, U. Mureddu, M. Laban, O. Petura, L. Bossuet and V. Fischer - *Hubert Curien Laboratory, U. of Lyon and Laboratoire Hubert Curien, U. of Saint-Etienne*
- *SPOILD: Side-channel POwer-based Instruction-Level Disassembler* F. Rahman, J. Park, X. Xu, D. Forte and M. Tehranipoor - *U. of Florida*
- *Hardware Trojan Detection through Electromagnetic Side-Channel Statistical Analysis: A Gold Chip Free Approach* J. He, X. Guo and Y. Jin - *U. of Central Florida*
- *Automatic Data Extraction from CBRAM and ReRAM Arrays* R. Chipana, B. Habib, B. Cambou and J. Taggart - *Northern Arizona U. and Arizona State University*
- *Leveraging Electromagnetic Emanations for IoT Security* N. Sehatbakhsh, R. Callan, M. Alam, M. Prvulovic and A. Zajic - *Georgia Institute of Technology*
- *IoTA: IoT Assurance* R. Pal, J. Clemens and B. Sherrell - *USG and JHU-APL*
- *A Processor + FPGA based Platform for Control Flow Integrity Enforcement* A. Iyengar, S. Ghosh and T. Jaeger - *Pennsylvania State U.*
- *Counterfeit IC Detection: A Defect Database and Test Procedure* M. M. Alam, S. Chowdhury, N. Asadizanjani, M. Tehranipoor and D. Forte - *U. of Florida*
- *Hardware Hacking Security Education Platform (HaHa SEP): Enabling Hands-On Applied Research of Hardware Security Theory & Principles* J. Vosatka, S. Yang, D. Forte and M. Tehranipoor - *U. of Florida*
- *Enhancing Power-Side-Channel-Attack Resistance via a Security-Aware Integrated*

Voltage Regulator M. Kar, A. Singh, S. Mathew, A. Rajan, V. De and S. Mukhopadhyay - *Georgia Institute of Technology and Intel*

- *Data Exfiltration using Building Automation to Bridge Air Gapped System* A. Mason, T. White, M. Talley, M. Tienteu, E. Ahovi, K. Kornegay, W. Thompson and D. Hamilton - *Morgan State University*
- *Spoofing, DOS, DDOS Attacks on a Z-Wave Home Automation System* L. S. M. Rao, K. Henderson, T. Yimer, A. Edmond, K. Kornegay and J. Ladeji-Osias - *Morgan State University*
- *Hacking Z-Wave using Insider Tools* A. Edmond, K. Henderson, L. Suryavanshi and T. Yimer - *Morgan State U*
- *UCR: An Unclonable Environmentally-Sensitive Chipless RFID Tag* K. Yang, H. Shen, D. Forte and M. M. Tehranipoor - *U. of Florida*
- *Demonstration of Built-in Secure Register Bank (BSRB) Protection Scheme for Embedded System Security* S. D. Kramer, Z. Zhang and Q. Yu - *U. of New Hampshire*
- *Prevention & Detection of Hardware Trojans in Wireless Cryptographic ICs: Silicon Demonstration* G. Volanis, C. Kapatsori, Y. Liu and Y. Makris - *U. of Texas at Dallas*
- *Real-time Causal Internet Log Analytics by HW/SW/Projection Co-design* B. D. Rouhani and F. Koushanfar - *U. of California San Diego.*
- *Demonstration of Hardware Trojan Attacks & Defenses in an IEEE 802.11a/g Network* K. S. Subramani, A. Antonopoulos, A. A. Abotabl, A. Nosratinia and Y. Makris - *U. of Texas at Dallas*
- *FAME: Fault Aware Microprocessor Extension Demonstrator* C. Deshpande, M. Ghodrati, B. Yuce, A. Bendre, C. Patrick, N. F. Ghalaty, L. Nazhandali and P. Schaumont - *Virginia Tech and Texas Tech.*
- *Practical Cryptographically-Secure PUFs based on Learning Parity with Noise* C. Jin, C. Herder, L. Ren, P. H. Nguyen, B. Fuller, S. Devadas and M. van Dijk - *U. of Connecticut and Massachusetts Institute of Technology*
- *Synthesis of Hardware Sandboxes for Trojan Mitigation in Systems on Chip* C. Bobda, T. JL Whitaker, C. Kamhoua, K. Kwiat and L. Njilla - *U. of Arkansas and Air Force Research Laboratory*
- *Hardware Based Secure CAN Bus Communication* A. S. Siddiqui, J. Plusquellic and F. Saqib - *Florida Institute of Technology and U. of New Mexico*
- *Implementation Diversity and Dynamic Partial Reconfiguration for Impeding Differential Power Analysis Attacks on FPGAs* N. G. Bete, M. Nakka, J. Plusquellic, F. Saqib, C. Patel and R. Robucci - *University of New Mexico, Florida Institute of Technology and U. of Maryland, Balt. Co.*
- *Ag Conductive Bridge RAMs for Physical Unclonable Functions* B. Cambou, F. Afghah, D. Sonderegger, J. Taggart, H. Barnaby and M. Kozicki - *Northern Arizona University and Arizona State University*