2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST 2016)

McLean, Virginia, USA
3-5 May 2016

IEEE Catalog Number: CFP16HOA-POD
ISBN: 978-1-4673-8827-6

******This publication is a representation of what appears in the IEEE Digital Libraries. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP16HOA-POD
ISBN (Print-On-Demand):	978-1-4673-8827-6
ISBN (Online):	978-1-4673-8826-9

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

Invited Visionary Talk	Gazing into the Hardware Security Crystal Ball
Date / Time	3 May 2016, Tuesday / 09:30 - 10:00
Speaker	**Kerry Bernstein**, *Defense Advanced Research Projects Agency (DARPA)*
Session Chair	**Ankur Srivastava**, *University of Maryland*

Biography

Kerry Bernstein joined DARPA in September 2012 as a program manager in the Microsystems Technology Office. His interests are in the areas of hardware assurance, hardware-based cybersecurity capabilities, and supply chain risk management, including anti-counterfeit and anti-tampering issues. His interests also include emerging post-CMOS device technologies for supporting future defense computing workloads. **Mr. Bernstein** came to DARPA from IBM's T.J. Watson Research Center where from 2002 until 2012 he was a research staff member working in the areas of high-performance, low-power devices, circuits and architectures; emergent post-CMOS logic switch technologies and architectures; 3D chip integration; and radiation-induced upset modeling. From 1978-2002, he was an electrical engineer at IBM Microelectronics working in microprocessor circuit design, high performance product development and technology development applications. Mr. Bernstein has co-authored four textbooks, holds 155 patents and is a Fellow of the IEEE. Mr. Bernstein received his Bachelor of Science degree in Electrical Engineering from Washington University in St. Louis.

Session 2	Hardware Authentication & PUF
Date / Time	3 May 2016, Tuesday / 10:30 - 12:10
Session Chair	**Arun Kanuparthi**, *Intel, USA*

- **Robust Privacy-Preserving Fingerprint Authentication**
  Ye Zhang and Farinaz Koushanfar

- **UCR: An Unclonable Chipless RFID Tag**
  Kun Yang, Domenic Forte and Mark M. Tehranipoor

- **A Highly Reliable and Tamper-Resistant RRAM PUF: Design and Experimental Validation**
  Rui Liu, Huaqiang Wu, Yachun Pang, He Qian and Shimeng Yu

- **Machine Learning Resistant Strong PUF: Possible or a Pipe Dream?**
  Arunkumar Vijayakumar, Vinay C. Patil, Charles B. Prado and Sandip Kundu

- **LEDPUF: Stability-Guaranteed Physical Unclonable Functions through Locally Enhanced Defectivity**
  Wei-Che Wang, Yair Yona, Suhas Diggavi and Puneet Gupta

Session	Lunch Talk : Because Failure is not an Option: Physical Unclonable Functions
Date / Time	3 May 2016, Tuesday / 12:30 - 13:10
Speaker	**Pim Tuyls**, *Founder and CEO, Intrinsic ID*

Session 3	Efficient Implementation of Secure Systems
Date / Time	3 May 2016, Tuesday / 13:30 - 15:10
Session Chair	**Shimeng Yu**, *Arizona State University*

- **Parsimonious Design Strategy for Linear Layers with High Diffusion in Block Ciphers**
  Sikhar Patranabis, Debapriya Basu Roy, Yash Shrivastava, Debdeep Mukhopadhyay and Santosh Ghosh

- **Iterating Von Neumann's Post-Processing under Hardware Constraints**
  Vladimir Rožić , Bohan Yang, Wim Dehaene and Ingrid Verbauwhede

- **Controlling Your Control Flow Graph**
  Arun Kanuparthi, Jeyavijayan Rajendran and Ramesh Karri

- **An Area-Optimized Serial Implementation of ICEPOLE Authenticated Encryption Schemes**
  Michael Tempelmeier, Fabrizio De Santis, Jens-Peter Kaps and Georg Sigl

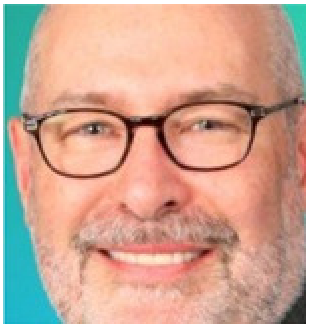
- **Round Gating for Low Energy Block Ciphers**
  Subhadeep Banik, Andrey Bogdanov, Francesco Regazzoni, Takanori Isobe, Harunaga Hiwatari and Toru Akishita

Session	Afternoon Keynote : Protecting Enterprise Data while in Use
Date / Time	3 May 2016, Tuesday / 15:10 - 15:40
Speaker	**Frank McKeen**, *Security Research Lab, Intel, USA*
Session Chair	**Yier Jin**, *University of Central Florida*

Abstract

Many organizations have fallen victim to the theft of confidential information and key business data. These thefts have significant business and personal impact. This talk will describe the requirements to protect data from rogue software while in use. It will also describe Intel's SGX, which provides such protections.

Biography



Frank McKeen Principal Engineer, Security Research Lab, Intel, Portland OR, USA. Frank is the inventor of the SGX architecture and leader of the SGX architecture research team. He has previous experience in microprocessor design, security concepts, and trusted computing. He received a BSEE from Northeastern University and is a member of the IEEE.

Session 4	Poster Session
Date / Time	3 May 2016, Tuesday / 15:40 - 17:00
Session Chair	**Qiaoyan Yu**, *University of New Hampshire*

- **Functional Polymorphism for Intellectual Property Protection**
  Jeffrey T. McDonald, Yong C. Kim, Todd R. Andel, James McVicar and Miles A. Forbes

- **The Conjoined Microprocessor**
  Ehsan Aerabi, A. Elhadi Amirouche, Houda Ferradi, Rémi Géraud, David Naccache and Jean Vuillemin

- **Low-Area Hardware Implementations of CLOC, SILC and AES-OTR**
  Subhadeep Banik, Andrey Bogdanov and Kazuhiko Minematsu

- **Functional Block Identification in Circuit Design Recovery**
  Jacob Couch, Elizabeth Reilly, Morgan Schuyler and Bradley Barrett

- **Robust Hardware True Random Number Generators using DRAM Remanence Effects**
  Fatemeh Tehranipoor, Wei Yan and John A. Chandy

- **Blinded Random Corruption Attacks**
  Rodrigo Branco and Shay Gueron

- **Trust Games: How Game Theory Can Guide the Development of Hardware Trojan Detection Methods**
  Jonathan Graf

- **ACBuilder: A Tool for Hardware Architecture Security Evaluation**
  Henrique Kawakami, David Ott, Hao-Chi Wong, Ricardo Dahab and Roberto Gallo

- **On the Problems of Realizing Reliable and Efficient Ring Oscillator PUFs on FPGAs**
  Alexander Wild, Georg T. Becker and Tim Güneysu

- **Model Checking to Find Vulnerabilities in an Instruction Set Architecture**
  Chris Bradfield and Cynthia Sturton

- **CryptoML: Secure Outsourcing of Big Data Machine Learning Applications**
  Azalia Mirhoseini, Ahmad-Reza Sadeghi and Farinaz Koushanfar

- **SDSM: Fast and Scalable Security Support for Directory-Based Distributed Shared Memory**
  Ofir Shwartz and Yitzhak Birk

- **Adaptive Real-time Trojan Detection Framework through Machine Learning**
  Amey Kulkarni, Youngok Pino and Tinoosh Mohsenin

- **Scalable SoC Trust Verification using Integrated Theorem Proving and Model Checking**
  Xiaolong Guo, Raj Gautam Dutta, Prabhat Mishra and Yier Jin

- **Information Leakage behind the Curtain: Abusing Anti-EMI Features for Covert Communication**
  Johannes Bauer, Sebastian Schinzel, Felix Freiling and Andreas Dewald

- **Granularity and Detection Capability of an Adaptive Embedded Hardware Trojan Detection System**
  Maxime Lecomte, Jacques J.A. Fournier and Philippe Maurine

- **Electronic Forensic Techniques for Manufacturer Attribution**
  Ryan L. Helinski, Edward I. Cole Jr., Gideon Robertson, Jonathan Woodbridge and Lyndon G. Pierson

- **Integrated All-Digital Low-dropout Regulator as a Countermeasure to Power Attack in Encryption Engines**
  A. Singh, M. Kar, A. Rajan, V. De and S. Mukhopadhyay

Session 5	Invited Industry Session : New Directions in Hardware Security
Date / Time	3 May 2016, Tuesday / 17:00 - 18:15
Session Chair	**Jim Plusquellic**, *University of New Mexico*

- **Enabling Supply Chain Security Assurance through an Authentication Data Network**
  Michael Schuldenfrei

- **Hardware-Assisted Cyber Security in Automotive Systems**
  Brian Murray

- **Efficient and Cost-Effective Testing for Side Channel Vulnerabilities**
  Mark Marson

Session 6	Plenary Session
Date / Time	4 May 2016, Wednesday / 7:45 - 8:45
Moderator	**Swarup Bhunia**, *University of Florida*

Keynote III	Technical Means to Detect Counterfeiting in the Real World: What the Government is Thinking, and How it is Driving Industry
Date / Time	4 May 2016, Wednesday / 08:45 - 09:30
Speaker	**Allan Steinhardt**, *Fellow and Senior Executive Advisor, Booz Allen Hamilton*
Session Chair	**Saverio Fazzari**, *Booz Allen Hamilton*

Abstract

The distinction between computer networks and networked disparate physical systems is blurring as we stand at the cusp of the IoT explosion.

In this overview we will survey trends in both vulnerabilities and technical solutions as well as prognosticate on some potential futures.

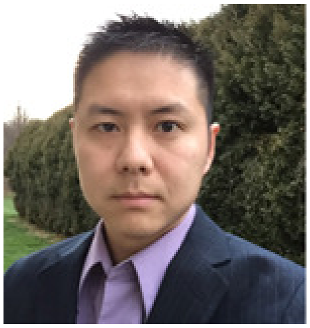
We will cover provably unclonable functions wireless signatures and related concepts.

Biography

Dr. Allan Steinhardt, a Booz Allen Hamilton Senior Executive Advisor, provides prototyping, portfolio analysis, technology roadmaps, and innovation services to the Office of the Secretary of Defense (OSD). Topics include: custom RF signal prototype collection systems for airborne platforms; prototype radar systems integration, signal processing, and concept of operations; physical and engineering sciences research management support; and science and technology subject matter expertise support for military intelligence. Prior to joining Booz Allen, Dr. Steinhardt served as a Program Manager, and later a Chief Scientist, at DARPA. He is a recipient of an IEEE teaching award, an IEEE paper award, an IEEE Fellow, and awardee of The Defense Medal for Exceptional Public Service, and of the OSD award for Outstanding Achievement. Dr Steinhardt is also a member of the National Academies' Naval Studies Board.

Invited Visionary Talk	HOST: HOST Oriented Security and Trust
Date / Time	4 May 2016, Wednesday / 09:30 - 10:00
Speaker	**Lok Yan**, *Air Force Research Lab, USA*
Session Chair	**Domenic Forte**, *University of Florida*

Biography



Dr. Lok Yan is a Senior Computer Engineer at the Air Force Research Laboratory, Information Directorate in Rome, NY. His research interests lie mainly at the crossroads between hardware, software and security. He received his Ph.D. from Syracuse University and is also an adjunct faculty at the Computer Science and Engineering department of New York University's Tandon School of Engineering.

Hardware Demos

Demo 1	Design Security Rule Check: Vulnerability Analysis for DFT Exploits of SoCs
Date / Time	4 May 2016, Wednesday / 10:05 - 11:00
Speaker	**Gustavo K. Contreras, Adib Nahiyan, Domenic Forte, and Mark Tehranipoor**, *U. of Florida, FL, USA*

Abstract

A major challenge with designing secure Systems-on-Chip (SoCs) is the diversity of existing and emerging attacks and potential countermeasures. A framework, called Design Security Rule Check (DSeRC), can be integrated in the conventional SoC design flow to analyze vulnerabilities of a design and assess its security at various stages of the design process, namely register transfer level (RTL), gate-level netlist, design-for-test (DFT) insertion, physical design, etc. The demonstration will show the automated vulnerability analysis tool in real-time.

Demo 2	A Strong-PUF Authentication Protocol for Resource-Constrained Devices
Date / Time	4 May 2016, Wednesday / 10:05 - 11:00
Speaker	**Wenjie Che and Jim Plusquellic**, *U. of New Mexico, NM, USA*

Abstract

The SHA-3 (keccakf200) secure hash algorithm is implemented on a Xilinx Zynq FPGA as a mechanism to implement a PUF-based authentication protocol. A hardware-embedded delay PUF called HELP integrates into the SHA-3 implementation to enable dual use of the functional unit, i.e., as a secure hash function and as a source of entropy for bitstrings used in the authentication protocol. A full client-server based authentication protocol, including enrollment, will be demonstrated between a set of FPGAs (tokens) and a secure server (a laptop).

Demo 3	A Low-Cost Portable Spectroscopic Device for Authentication of Medicines and Food Products
Date / Time	4 May 2016, Wednesday / 10:05 - 11:00
Speaker	**Cheng Chen**, *Case Western Reserve U., OH, USA* **Fengchao Zhang**, *U. of Florida, FL, USA* **Soumyajit Mandal**, *Case Western Reserve U., OH, USA*

Abstract

A chemometric passport approach is demonstrated for authenticating pharmaceutical supply chain medicines as a means of providing quality assurance and addressing public health issues.

Demo 4	ReSC: An RFID-Enabled Solution for Defending IoT Supply Chain
Date / Time	4 May 2016, Wednesday / 10:05 - 11:00
Speaker	**Kun Yang, Domenic Forte and Mark M. Tehranipoor**, *U. of Florida, FL, USA*

Abstract

An RFID-enabled technique is demonstrated that aims at defending the IoT supply chain by addressing two major issues including the disappearance/theft of authentic IoT devices and appearance of counterfeit IoT devices.

Demo 5	Hardware Trojans in Wireless Cryptographic ICs: Silicon Demonstration & Detection Evaluation
Date / Time	4 May 2016, Wednesday / 10:05 - 11:00
Speaker	**Yu Liu and Yiorgos Markis**, *The U. of Texas at Dallas, TX, USA*

Abstract

The threat of hardware Trojans in wireless cryptographic ICs, as well as the effectiveness of two detection methods, is demonstrated using a custom-designed chip consisting of an Advanced Encryption Standard (AES) core and an Ultra-Wide-Band (UWB) transmitter.

Demo 6	Firmware Instruction Identification Using Side-Channel Power Analysis
Date / Time	4 May 2016, Wednesday / 10:05 - 11:00
Speaker	**Chintan Patel and Ryan Robucci**, *U. of Maryland, Baltimore County, MD, USA*

Abstract

A side-channel analysis is performed over multiple power supply pins to demonstrate the relationship between the power transients and machine-level instructions on an instance of the openMSP430 processor on an FPGA.

Demo 7	Configurable Ring Oscillator PUF as an Entropy Pump
Date / Time	4 May 2016, Wednesday / 10:05 - 11:00
Speaker	**Qian Wang and Gang Qu**, *U. of Maryland, MD, USA*

Abstract

A silicon physical unclonable function (PUF) is used as an entropy source to enhance a random input string. This is accomplished by using an input random string as the configuration vector for the flexible ring oscillator (RO) PUF which generates another random string (the PUF bits).

Demo 8	Multi-Communication Type Debugging Probe
Date / Time	4 May 2016, Wednesday / 10:05 - 11:00
Speaker	**Austin Funes, Cheng Guo, Somtochukwu Okwuosah, Fatemeh Tehranipoor and John Chandy**, *U. of Connecticut, CT, USA*

Abstract

A Multi-Communication Type Debugging (MCTD) probe is demonstrated, which is capable of identifying the test pins on a PCB and for auto-detecting the communication protocol being used by the device with only a small amount of information available to the user.

Demo 9	Robotic Arm based CPS Security Platform
Date / Time	4 May 2016, Wednesday / 10:05 - 11:00
Speaker	**Kelvin Ly and Yier Jin**, *U. of Central Florida, FL, USA*

Abstract

A robotic arm system is demonstrated that can be used as a testbed for CPS security and the related fields in robust and cooperative control systems. The arms are connected together in a wireless network, allowing for remote programming and message passing between the arms themselves. Some simple tasks are demonstrated to allow performance to be benchmarked.

Demo 10	Potential Pitfall of RLUT: Fault Attack using Hardware Trojan
Date / Time	4 May 2016, Wednesday / 10:05 - 11:00
Speaker	**Debapriya Basu Roy, Shivam Bhasin, Sikhar Patranabis, Sylvain Guilley, Jean-Luc Danger, Debdeep Mukhopadhyay, Xuan Thuy Ngo and Zakaria Najm**, *Telecom ParisTech, Paris, France*

Abstract

Dynamic reconfiguration via a look-up table (RLUT) in modern FPGAs allows users to modify the functionality of LUTs at runtime. This hardware demonstration shows a stealthy hardware Trojan in an untrusted IP vendor attack scenario.

Demo 11	Quantified Analysis of Magnetic Attack on Commercial Magnetic RAM Chip
Date / Time	4 May 2016, Wednesday / 10:05 - 11:00
Speaker	**Alexander Holst and Swaroop Ghosh**, *U. of South Florida, FL, USA*

Abstract

Magnetoresistive random-access memory (MRAM) is a prime candidate to become a universal memory to serve all requirements for information storage, from short-term to long-term. This demonstration will show the vulnerability of MRAM to externally-applied static magnetic fields by correlating the magnetic field strength with the gross error rate observed on a commercial MRAM chip.

Demo 12	Prototype Demonstration of Secure Control Area Network (CAN) against Masquerade and Replay Attacks
Date / Time	4 May 2016, Wednesday / 10:05 - 11:00
Speaker	**Mohammad Raashid Ansari, Qiaoyan Yu and Tom Miller**, *U. of New Hampshire, NH, USA*

Abstract

CAN is one of the widely used communication buses in an automobile to connect electronic control units (ECUs). The design of the CAN protocol renders it defenseless against emerging masquerade and replay attacks. This hardware demonstration investigates hardware/firmware-level methods to detect and mitigate these types of attacks.

Demo 13	Charging Battery for Information Leakage
Date / Time	4 May 2016, Wednesday / 10:05 - 11:00
Speaker	**Khoa Hoang, Jacob Wurm and Yier Jin**, *U. of Central Florida, FL, USA*

Abstract

A charging battery of an iPhone or Android phone is modified in this hardware demonstration to include malicious components that can control the smart phone to do anything such as making phone calls, download apps, etc.

Demo 14	Demonstration of a Hardware Trojan Attack in an IEEE 802.11a/g Network
Date / Time	4 May 2016, Wednesday / 10:05 - 11:00
Speaker	**Kiruba S. Subramani, Angelos Antonopoulos, Aria Nosratinia, and Yiorgos Makris**, *The U. of Texas at Dallas, TX, USA*

Abstract

Wireless networks are now prevalent in sensor applications and the Internet of Things. Even though wireless devices use some form of encryption, the underlying hardware is still vulnerable to hardware Trojans. This hardware demonstration (i) describes the risks posed by hardware Trojans in wireless networks (ii) elucidate the risk by developing realistic attacks (iii) demonstrate attacks on experimental platforms and (iv) develop defense mechanisms.

Demo 15	Flexible, Opensource workbench for Side-channel analysis (FOBOS)
Date / Time	4 May 2016, Wednesday / 10:05 - 11:00
Speaker	**Rajesh Velegalati, Panasayya Yalla and Jens-Peter Kaps**, *George Mason U., VA, USA*

Abstract

Side-channel analysis attacks pose a grave threat to implementations of cryptographic algorithms implemented in software as well as in hardware. The demonstrated FOBOS technique simplifies the task of carrying out side-channel attacks by supporting multiple FPGA devices, and including all necessary software to run differential power analysis attacks, which are the most prominent kind of side-channel attacks.

Session 8	Attacks & Forensics
Date / Time	4 May 2016, Wednesday / 11:00 - 12:00
Session Chair	**Wujie Wen**, *Florida International University*

- **A Layout-driven Framework to Assess Vulnerability of ICs to Microprobing Attacks**
  Qihang Shi, Navid Asadizanjani, Domenic Forte and Mark M. Tehranipoor

- **A New Approach for Rowhammer Attacks**
  Rui Qiao and Mark Seaborn

- **Hardware-based Workload Forensics: Process Reconstruction via TLB Monitoring**
  Liwei Zhou and Yiorgos Makris

Session	Lunch Talk : Strong PUF-based Authentication for IoT and Beyond
Date / Time	4 May 2016, Wednesday / 12:30 - 13:00
Speaker	**Jim Plusquellic**, *CTO, Charles E. Mendez Jr., CEO, Enthentica*

Session 9	System Security: Risk Analysis & Solutions
Date / Time	4 May 2016, Wednesday / 13:20 - 15:00
Session Chair	**Ioannis Savidis**, *Drexel University*

- **A Key-centric Processor Architecture for Secure Computing**
  David Whelihan, Kate Thurmer and Michael Vai

- **Hardware Security Risk Assessment: A Case Study**
  Brent Sherman and David Wheeler

- **A Novel Security Technique to Generate Truly Random and Highly Reliable Reconfigurable ROPUF-based Cryptographic Keys**
  Fathi Amsaad, Atul Prasad Deb Nath, Chayanika Roychaudhuri and Mohammed Niamat

- **A Zero-cost Approach to Detect Recycled SoC Chips Using Embedded SRAM**
  Zimu Guo, Md. Tauhidur Rahman, Mark M. Tehranipoor and Domenic Forte

- **Redirecting DRAM Memory Pages: Examining the Threat of System Memory Hardware Trojans**
  Bradley Hopkins, John Shield and Chris North

Session 10	Side Channels: The Good and the Bad
Date / Time	4 May 2016, Wednesday / 15:20 - 16:20
Session Chair	**Fareena Saqib**, *Florida Institute of Technology*

- **Large Laser Spots and Fault Sensitivity Analysis**
  Falk Schellenberg, Markus Finkeldey, Nils Gerhardt, Martin Hofmann, Amir Moradi and Christof Paar

- **The Other Side of The Coin: Analyzing Software Encoding Schemes Against Fault Injection Attacks**
  Jakub Breier, Dirmanto Jap and Shivam Bhasin

- **IP Core Protection using Voltage-Controlled Side-Channel Receivers**
  Peter Samarin, Kerstin Lemke-Rust and Christof Paar

Session 11	Panel I : Hardware-Enabled System Security
Date / Time	4 May 2016, Wednesday / 16:20 - 17:50
Panel Moderator	**Mark Tehranipoor**, *University of Florida*

Abstract

his panel will focus on the role of hardware in driving system security, including security of the software stack and zillion applications running in a system. With new application spaces emerging, such as internet-of-things (IoT) and connected autonomous cars, hardware is poised to play increasingly important roles in designing secure systems. On the other hand, new security issues in hardware question the fundamental assumptions on hardware root of trust. How we deal with these issues to build secure hardware trust anchors? A distinguished set of speakers in this panel will share their viewpoints on these issues and take us to the future.

Panelists:

- **Tony Jeffs**, *Cisco Systems*
- **Tom Tkacik**, *NXP Semiconductor*
- **Jim Fahrny**, *Comcast*
- **Ethan Cannon**, *Boeing*
- **Serge Leef**, *Mentor Graphics*

Session 12	Plenary Session
Date / Time	5 May 2016, Thursday / 7:45 - 8:45
Moderator	**Ryan Kastner**, *University of California, San Diego*

Keynote IV	From Star Trek to Star Wars: The Force Awakens - The Importance of Hardware and IP Security
Date / Time	5 May 2016, Thursday / 08:45 - 09:30
Speaker	**Carl E. McCants**, *Intelligence Advanced Research Projects Activity (IARPA)*
Session Chair	**Gang Qu**, *University of Maryland*

Biography

Dr. Carl E. McCants received the B.S.E. degree from Duke University, Durham, NC in 1981 and the M.S. and Ph. D. degrees from Stanford University, Stanford, CA in 1982 and 1989, respectively, all in electrical engineering. His doctoral research focused on using photoemission spectroscopy to study metal/III-V semiconductor interface development, and correlate interfacial chemistry with macroscopic electrical properties. He is currently a Program Manager at the Intelligence Advanced Research Projects Activity (IARPA) in the Office of Safe and Secure Operations, and is managing the Rapid Analysis of Various Emerging Nanoelectronics (RAVEN) program, the Circuit Analysis Tools (CAT) program and the Trusted Integrated Chips (TIC) program. From 2010 to 2012, he was a Program Manager in the Defense Advanced Research Projects Agency (DARPA) Microsystems Technology Office (MTO), focused on microelectronic integration and hardware assurance and reliability. The programs he managed included the Integrity and Reliability of Integrated Circuits (IRIS) program, the Trust in Integrated Circuits (TRUST) program, the Gratings of Regular Arrays and Trim Exposures (GRATE) program, the Leading Edge Access Program (LEAP), and the 3-Dimensional Integrated Circuits (3DIC) program.

From 2003 to 2009 he was an Associate at Booz Allen Hamilton, Arlington, VA, where he served as the Chief Technologist to the Director of the MTO Office, and Special Assistant to the Deputy Director, DARPA. From 1999 to 2003 he was a Project Manager at Agilent Technologies' Semiconductor Products Group, San Jose, CA, where he was responsible for front-end and back-end optical and electrical characterization of VCSEL-based devices and transceivers, and automated test platform development. From 1988 to 1999 he was a Development Engineer at Hewlett-Packard's Optical Communication Division, where he focused on III-V materials characterization, wafer fabrication and die-level photonic measurements for NIR and SWIR LEDs and lasers. Dr. McCants is a Senior Member of IEEE. He is also a member of the Board of Visitors for the Pratt School of Engineering at Duke University.

Invited Visionary Talk	Cybersecurity Today and Tomorrow: Assurance or Insurance?
Date / Time	5 May 2016, Thursday / 09:30 - 10:00
Speaker	**Apostol Vassilev**, *Technical Director, National Institute of Standards and Technology (NIST)*
Session Chair	**Greg Creech**, *Assistant Director, Electroscience Lab, USA*

Biography

Dr. Vassilev is the Research Lead in the Security Testing Validation & Measurement Group at NIST. He leads research in testing methodologies and standards for cryptographic implementations and works with industry, academia and government agencies to develop and promote better cybersecurity testing and measurement.

Dr. Vassilev holds a Ph.D. in Mathematics from Texas A&M University. He holds six US patents and has authored over thirty scientific papers.

Session 13	Attack-Resistant Design and Protocols
Date / Time	5 May 2016, Thursday / 10:30 - 12:10
Session Chair	**Aaron E. Cohen**, *NRL, Washington, DC*

- **A Separation and Protection Scheme for On-Chip Memory Blocks in FPGAs**
  Luis Ramírez Rivera, Xiaofang Wang and Danai Chasaki

- **A Secure Camouflaged Threshold Voltage Defined Logic Family**
  Burak Erbagci, Cagri Erbagci, Nail Etkin Can Akkaya and Ken Mai

- **SARLock: SAT Attack Resistant Logic Locking**
  Muhammad Yasin, Bodhisatwa Mazumdar, Jeyavijayan (JV) Rajendran and Ozgur Sinanoglu

- **Template Attacks using Classification Algorithms**
  Elif Özgen, Louiza Papachristodoulou and Lejla Batina

- **GenMatch: Secure DNA Compatibility Testing**
  M. Sadegh Riazi, Neeraj K. R. Dantu, L. N. Vinay Gattu and Farinaz Koushanfar

Session 14	Panel II : Hardware IP Protection Through Invasive and Non-Invasive Analysis
Date / Time	5 May 2016, Thursday / 13:10 - 14:40
Panel Moderator	**Saverio Fazzari**, *Booz Allen Hamilton*

Abstract

This panel will focus on emerging security and trust issues in hardware IPs, accentuated by the evolving semiconductor business landscape that promotes extensive outsourcing and distributed global supply chain. These IPs are increasingly subject to various security issues for all parties concerned. How do we address these issues in meaningful ways? A distinguished set of speakers in this panel will share their viewpoints on these issues and beyond.

Panelists:

- **Edward Principe**, *Tescan USA Inc.*
- **Yier Jin**, *University of Central Florida*
- **Chris Pawlowicz**, *TechInsights*
- **Len Orlando**, *Air Force Research Lab*
- **Steve Trimberger**, *Xilinx*
- **Matthew Scholl**, *NIST*