Cyber Physical Systems Security (CPSSEC)
Principal Investigator Meeting

February 23-24, 2017

Phyllis P. Marshall Student Center, MSC 4200 “The Chamber”
University of South Florida, Tampa, FL
http://cpssec.arguslab.org/

Thursday, February 23, 2017

8:00 am	Registration
8:10 am	DHS Welcome, Purpose, Agenda, and Ground Rules - **Dr. Dan Massey, DHS S&T**
8:15 am	University of South Florida Welcome and Overview – **Dr. Robert H. Bishop, Dean of College of Engineering, Dr. Sudeep Sarkar, Chair of CSE Dept.**
8:30 am	CPSSEC Program Overview and Update – **Dr. Dan Massey and Chase Garwood, DHS S&T**
8:45 am	CPSSEC Project Team Introductions
10:15 am	Break
10:30 am	Building Controls: Modeling security/safety interactions in buildings for compositional security/safety control – **Dr. Simon Ou, U. of South Florida**
10:55 am	Medical: MDRAP: Medical Device Risk Assessment Platform – **Dr. Dale Nordenberg, MDISS**
11:20 am	Medical: ISOSCELES: Intrinsically Secure, Open, and Safe Control of Essential LayErs – **Todd Carpenter, Adventium Labs**
11:45	Automotive: Securely Updating Automobiles – **Trishank Karthik and Dr. Justin Cappos, NYU**
12:10 pm	Lunch: Box Lunches will be ordered
1:30 pm	Automotive: Secure Software Update Over-the-Air for Ground Vehicles Specification and Prototype – **Sam Lauzon, UMTRI**
1:55 pm	Automotive: Side-Channel Causal Analysis for Design of Cyber-Physical Security – **David Payton, HRL**
2:20 pm	DOT/DHS: Joint Agency Work on Automotive Cyber Security – **Kevin Harnett, DOT Volpe**
2:45 pm	Secure Microkernels and seL4 – **Dr. Gernot Heiser, Data61, CSIRO**
3:10 pm	Break
3:30 pm	Technology Demonstrations (Part 1 of 2) 3:30 University of South Florida 3:50 MDISS 4:10 HRL and UC Irvine

	4:30 UPTANE – NYU 4:45 UPTANE - UMTRI
5:00 pm	Adjourn
6:00 pm	No Host Dinner at Stonewood Grill: 17070 Palm Pointe Dr., Tampa, FL

Friday, February 24, 2017

8:00 am	Registration
8:15 am	Review Purpose and Agenda – **Dr. Dan Massey and Chase Garwood, DHS S&T**
8:30 am	NSF/DHS: High-Fidelity, Scalable, Open-Access Cyber Security Testbed for Accelerating Smart Grid Innovations and Deployments – **Dr. Manimaran Govindarasu, Iowa State University**
8:55 am	NSF/DHS: A Verifiable Framework for Cyber-Physical Attacks and Countermeasures in a Resilient Electric Power Grid – **Dr. Lalitha Sankar, Arizona State University**
9:20 am	NSF/DHS: Cyber Security for Smart Manufacturing – **Dr. Christopher Williams, Virginia Tech**
9:45 am	NSF/DHS New Start: Support for Security and Safety of Programmable IoT Systems - **Dr. Atul Prakash, University of Michigan**
10:00 am	Break
10:30 am	DHS S&T Related Programs: A Mission Impact Situational Awareness Tool for Distributed Operations Management of Cyber-Physical-Human Critical Infrastructures – **Dr. Sandip Roy, Washington State University**
10:55 am	DHS S&T Related Programs: Project Ares Operational Ocean View – **Keenan Skelly, Circadence**
11:20 pm	Program Manager Panel: **DHS S&T, NSF, and UK**
11:45 am	Working Lunch and Technology Demonstrations (Part 2 of 2) 11:45 Brigham Young University 12:05 Iowa State University 12:25 Arizona State University 12:45 Vanderbilt and Virginia Tech 1:05 Adventium Labs 1:25 Circadence
1:45 pm	Milestones, Requirements, and Wrap-Up – **Dr. Dan Massey, Chase Garwood, Tammi Fisher, Mario Ayala, DHS S&T, and David Balenson, SRI International**
2:00 pm	Adjourn

CPSSEC Management Team Photos and Bios

Dr. Doug Maughan, DHS S&T CSD

Dr. Douglas Maughan is the Cyber Security Division Director in the Homeland Security Advanced Research Projects Agency (HSARPA) within the Science and Technology (S&T) Directorate of the Department of Homeland Security (DHS). Dr. Maughan has been at DHS since October 2003 and is directing and managing the Cyber Security Research and Development activities and staff at DHS S&T. His research interests and related programs are in the areas of networking and information assurance. Prior to his appointment at DHS, Dr. Maughan was a Program Manager at the Defense Advanced Research Projects Agency (DARPA) in Arlington, Virginia. Prior to his appointment at DARPA, Dr. Maughan worked for the National Security Agency (NSA) as a senior computer scientist and led several research teams performing network security research. Dr. Maughan received Bachelor's Degrees in Computer Science and Applied Statistics from Utah State University, a Masters degree in Computer Science from Johns Hopkins University, and a PhD in Computer Science from the University of Maryland, Baltimore County (UMBC).

Dr. Dan Massey, DHS S&T CSD

Dan Massey is a program manager in the Cyber Security Division, Science and Technology Directorate, US Department of Homeland Security. At DHS, his portfolio includes Distributed Denial of Service Defense (DDoSD), security for Cyber Physical Systems (CPSSEC), Secure Protocols for Routing Infrastructure (SPRI), and Homeland Open Security Technology (HOST). Prior to joining DHS, Dr. Massey was a tenured associate professor at Colorado State University and served as a PI on research funded by DHS, DARPA, and NSF. Some of his projects have included the Named Data Networking project that is developing a new information centric architecture, editor for the DNS Security Extensions (DNSSEC), internet BGP monitoring and analysis, and infrastructure security enhancements such as the Route Origin Verifier. He earned his bachelor's degree in mathematics and computer science and master's degree in applied mathematics all from the University of California, San Diego and his doctorate in computer science from the University of California, Los Angeles.

Chase Garwood, DHS S&T CSD

Chase Garwood is a program manager in the Cyber Security Division for the Homeland Security Advanced Research Projects Agency (HSARPA) at DHS S&T. He manages programs in cyber physical systems and national critical infrastructure. Before joining CSD, he managed programs supporting emergency management and infrastructure protection. Prior to his positions in S&T, he had over 16 years of federal information technology experience working in multiple Chief Information Officer (CIO), Deputy-CIO, and Chief Technology Officer positions in DHS operational components and other federal agencies. Key highlights include his work in the Student and Exchange Visitor and US-VISIT programs. While in the National Protection and Programs Directorate's CIO office, he was responsible for establishing the National Cybersecurity and Communications Integration Center. He previously served in the United States Army with the 3rd Armored Cavalry Regiment and in the Army Reserves with the 450th Civil Affairs Battalion (Airborne). Mr. Garwood holds a Bachelor of Science degree in Management from the University of Florida, a Juris Doctor from Ohio Northern University, an e-Commerce Graduate Certificate from the University of Virginia, and a Federal CIO Certification from Carnegie Mellon University.

Dr. David Corman, NSF

Dr. David Corman is the Program Director leading the Cyber Physical Systems Program for the National Science Foundation. He is also involved in the Innovations at the Nexus of Food, Energy, and Water (INFEWS) program, and NSF's Smart and Connected Community research. Dr. Corman obtained a dual BS degree in System Science and Mathematics and Applied Mathematics and Computer Science from Washington University in 1977. He then obtained a dual MS degree in SSM and Mechanical Engineering from Washington University in 1978. He completed his graduate education at the University of Maryland – College Park, and obtained a PhD in Electrical Engineering in 1983 with a major in controls and minor in communications. While at Maryland. Dr. Corman also worked at the Johns Hopkins Applied Physics Laboratory in the area of estimation, detection, and control. He worked for McDonnell Douglas / Boeing in a variety of positions. His work included a broad portfolio of DARPA and Air Force Research Laboratory research programs. He was elected a Boeing Technical Fellow in 1999. Dr. Corman joined NSF's Computer and Information System Engineering (CISE) directorate as an IPA in March 2013 as a Senior Research Scientist with the University of Maryland's Institute for Systems Research. He was appointed as a Research Associate Professor in the Preston M. Green Department of Electrical & Systems Engineering at Washington University in St. Louis, in March 2015. Dr. Corman's current research interests are in the field of Cyber Physical Systems (CPS), security for CPS, unmanned systems, and manufacturing. Dr. Corman has approximately 30 publications and has obtained five patents.

Tammi Fisher, DHS S&T CSD

Tammi Fisher provides SETA (contract) support to Dr. Dan Massey within the Cyber Security Division, Science and Technology Directorate, US Department of Homeland Security. Tammi has been providing programmatic support at DHS S&T for the past 12 years. At DHS, her portfolio includes Distributed Denial of Service Defense (DDoSD), Cyber Physical Systems Security (CPSSEC), Secure Protocols for Routing Infrastructure (SPRI), and Homeland Open Security Technology (HOST). Ms. Fisher has supported DHS for over twelve years. In addition to supporting efforts within the CSD portfolio, she is a Senior Associate with BayFirst Solutions and provides management to BayFirst staff throughout the Science and Technology (S&T) directorate.

Mario Ayala, DHS S&T CSD

Mario Ayala joined DHS Science and Technology Directorate (S&T) from the National Protection and Programs Directorate's (NPPD) Office of Cybersecurity and Communications (CS&C) in support of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). At ICS-CERT, Mario was responsible for coordinating all of ICS-CERT's onsite cybersecurity assessment activities. Mario coordinated over 252 onsite assessments across the 16 critical infrastructure (CI) sectors, which assisted asset owners in evaluating their control system architecture and cybersecurity posture. Mario also identified opportunities to strategically engage with DHS entities such as the Regional Protective Security Advisors (PSA) and Cybersecurity Advisors (CSA). At ICS-CERT, Mario pioneered a comprehensive performance metric tracking and reporting mechanism. Mario graduated from the George Mason University School of Business with a B.S. in Information Systems and Operations Management (ISOM).

David Balenson, SRI International

David Balenson is a Senior Computer Scientist in the Computer Science Laboratory at SRI International where he provides technical and programmatic support for the U.S. Department of Homeland Security Science and Technology Directorate (DHS S&T) cybersecurity R&D program, including the Cyber Physical Systems Security (CPSSEC), Transition to Practice (TTP), and other projects. He has more than 35 years of technical cybersecurity experience, and more than 15 years of management experience. Mr. Balenson is an energetic and highly motivated professional with the ability to drive research programs and organizations to research, develop, test, and evaluate innovative solutions to challenging cybersecurity needs and requirements. He received his B.S. and M.S. in Computer Science from the University of Maryland.

Funded Effort Speaker Photos and Bios

Todd Carpenter, Adventium Labs

Mr. Carpenter is Chief Engineer and co-owner of Adventium Labs. His areas of expertise include engineering high-value, real-time, fault-tolerant, and secure systems in space, military and commercial avionics, medical, and petrochemical domains. His expertise spans detailed hardware and software design, architecture development, systems design and specification, as well as tools, standards, and processes for enhancing design flows. Current activities include developing architectures for safe and secure medical devices, and developing fault management techniques and remote, dynamic, incremental attestation for distributed systems. Mr. Carpenter leads Adventium's risk assessment and management services, which evaluates, and teaches how to evaluate, security risk for cyber physical systems and products in medical, avionics, and industrial domains.

Dr. Dale Nordenberg, MDISS

Dr. Nordenberg is the co-founder and Executive Director for the Medical Device Innovation, Safety, and Security Consortium (MDISS), a public-private partnership that works closely with leading device manufacturers, healthcare systems, government agencies, and other stakeholders to improve the security and safety of medical devices from design through retirement. In addition, Dr. Nordenberg is CEO of Novasano Health and Science and also cofounded and co-directs the public-private partnership, TBResist. Prior to Novasano, Dr. Nordenberg was a managing director in the health care practice of PricewaterhouseCoopers. From 2002 through 2007, Dr. Nordenberg held various positions at CDC and was detailed to the Office of the National Coordinator for Health Information Technology at HHS in 2004-5 to catalyze the development of a national strategy for children's health information technology. Dr. Nordenberg is a board certified pediatrician, medical epidemiologist, and medical informaticist. He received a BS in Microbiology from the University of Michigan, his medical degree from Northwestern University, completed his training in pediatrics at McGill University, Montreal Children's Hospital, and his fellowship in epidemiology and public health in the Epidemic Intelligence Services Program at the Centers for Disease Control with a focus on 'big data'.

Dr. Justin Cappos, New York University

Justin Cappos is an assistant professor at NYU in the Tandon School of Engineering. Justin's research interests generally fall broadly in the area of systems security. He focuses on understanding high-impact, large-scale problems by building and measuring deployed systems. Prof. Cappos did his dissertation work describing flaws in prior Linux package managers and building / deploying a new security model. His work on software update system security was deployed by the major Linux package managers (e.g. apt, yum, pacman, and YaST), and thus protects most Linux servers. His more recent work on software updaters has been standardized by Python and deployed by Docker. He has fixed fundamental security design flaws in other widely used software, including git. Justin also created the Seattle testbed, a networking testbed with tens of thousands of installs and thousands of users. Due to the practical impact of his research, Prof. Cappos was named in 2013 as one of Popular Science's Brilliant 10 scientists under 40.

Trishank Karthik, New York University

Trishank Karthik Kuppusamy is a 5th year PhD student at the NYU Tandon School of Engineering where he works with Prof. Justin Cappos on software update security. He led the specification for Uptane, which aims to secure software updates for automobiles. He also worked on improving the security and efficiency of The Update Framework (TUF), a predecessor to Uptane, which is now used in Docker, Flynn, and LEAP, and is being integrated by CoreOS, Haskell, OCaml, Python, and Ruby. He likes to lift weights in his free time.

Sajcm Lauzon, University of Michigan

Sam has over ten years of embedded electronics experience in both the automotive and security industries. After completing a Bachelor's degree in Electronics Engineering Technology, Sam started in the security industry by designing and implementing custom interfaces integrating standard industrial controls and SCADA systems with proprietary monitoring and access platforms. In 2012, Sam began work at Harman International developing vehicle interface software used in Fiat/Chrysler infotainment systems worldwide. Two years later, Sam transitioned to a systems engineering role where he led the implementation of an infotainment product’s over-the-air software update mechanism. In December of 2015, Sam joined the UMTRI Cyber-security group where he is the technical leader of the DHS Project for Secure Software Update Over the Air for Ground Vehicles. Sam is also involved in investigating vehicle data bus security and vehicle intrusion detection.

David Payton, HRL Laboratories

David Payton is Principal Research Scientist in the Information and Systems Sciences Lab at HRL Laboratories in Malibu, California. Mr. Payton holds an MS degree in EE & CS from MIT and a BS degree in Electrical Engineering from UCLA. He has previously served as lead scientist for the DARPA Physical Intelligence project, and has been principal investigator for the DARPA Pheromone Robotics project, and the DARPA Neuro-robotic Perception and Control program. He is currently involved in research related to autonomous robots, machine learning, complex systems, and resilience, and is participating in the DARPA UPSIDE program for development of a high-performance image processing pipeline using novel emerging devices. After joining HRL Laboratories in 1982, Mr. Payton has been involved in numerous projects for the development of intelligent autonomous agents. This includes work on the

DARPA Autonomous Land Vehicle project, the Unmanned Ground Vehicle, the development of behavior-based robot control. More recently, he has led the development of imitation learning in humanoid robots for General Motors. Mr. Payton has over 30 publications and holds 26 patents.

Dr. Simon Ou, University of South Florida

Dr. Xinming (Simon) Ou is currently associate professor of Computer Science and Engineering at University of South Florida. He received his PhD from Princeton University in 2005. Before joining USF in fall 2015, he had been a faculty member at Kansas State University since 2006. Dr. Ou's research is primarily in cyber defense technologies, with focuses on intrusion/forensics analysis, cloud security and moving-target defense, mobile system security, and cyber physical system security. His MulVAL attack graph tool has been used by Idaho National Laboratory, Defence Research and Development Canada -- Ottawa, NATO, NIST, Thales Groups, General Dynamics, Johns Hopkins University Applied Physics Lab, and by researchers from numerous academic institutions. Dr. Ou's research has been funded by U.S. National Science Foundation, Department of Defense, Department of Homeland Security, Department of Energy, National Institute of Standards and Technology (NIST), HP Labs, and Rockwell Collins. He is a recipient of 2010 NSF Faculty Early Career Development (CAREER) Award, a three-time winner of HP Labs Innovation Research Program (IRP) award, and 2013 Kansas State University Frankenhoff Outstanding Research Award.

Kevin Harnett, DOT Volpe National Transportation Systems Center

Kevin Harnett is a Program Manager for the United States Department of Transportation (DOT) at the Volpe National Transportation Systems Center located in Cambridge, Massachusetts. Mr. Harnett has over 36 of combined project management, technical consulting, and implementation skills. Kevin is a Cybersecurity Program Manager (PM) with experience providing technical leadership in planning, implementing and managing high priority programs involving Cybersecurity and risk management for the DOT, Federal Aviation Administration (FAA), National Highway and Traffic Safety (NHTSA), DOD/USAF, Defense Information Systems Agency (DISA), NASA, DHS, and other agencies. Since 2010, Kevin has supported NHTSA on their “Research Planning for Cybersecurity of Automotive Safety-Critical Electronic Control Systems” Program and the development of a Vehicle Cybersecurity Threat/Risk Model, Assessment of the Automotive Information Sharing and Analysis Center (Auto ISAC) Model Paper, Vehicle Cybersecurity Testing laboratory, and Vehicle Cybersecurity Guidance. Since October 2014, Kevin has supported DHS S&T CSD on three major programs focusing on automotive cybersecurity: Automotive Cybersecurity Industry Consortium (ACIC) and Cybersecurity for Government Vehicles Program and Automotive Cybersecurity Tools Research. In support of DHS and NHTSA, Kevin has been evaluating OBD-2 dongles/telematics systems, CAN Bus, Bluetooth, etc. and state-of-the-art Automotive Cybersecurity countermeasures, such as Intrusion Detection System (IDS), Intrusion Prevention Systems (IPS), Firewalls, etc.) in the Volpe Cybersecurity Vehicle Testing Lab.

Dr. Jules White, Vanderbilt University

Dr. White is an Assistant Professor of Computer Science in the Dept. of Electrical Engineering and Computer Science at Vanderbilt University. He is a National Science Foundation CAREER Award recipient. He was previously a faculty member in Electrical and Computer Engineering at Virginia Tech and won the Outstanding New Assistant Professor Award at Virginia Tech. His research has won 4 Best Paper Awards. He has also published over 110 papers. Dr. White's research focuses on securing, optimizing, and leveraging data from mobile cyber-physical systems. His mobile cyber-physical systems research spans four key focus areas: (1) mobile security and data collection, (2) IoT security, (3) mobile device and supporting cloud infrastructure power and configuration optimization, and (4) applications of mobile cyber-physical systems in multi-disciplinary domains, including energy-optimized cloud computing, smart grid systems, healthcare/manufacturing security, next-generation construction technologies, and citizen science. His research has been licensed and transitioned to industry, where it won an Innovation Award at CES 2013, attended by over 150,000 people, was a finalist for the Technical Achievement at Award at SXSW Interactive, and was a top 3 for mobile in the Accelerator Awards at SXSW 2013. His research is conducted through the Mobile Application computinG, optimizatoN, and secUrity Methods (MAGNUM) Group at Vanderbilt University, which he directs.

Dr. Manimaran Govindarasu, Iowa State University

Dr. Manimaran Govindarasu is currently Mehl Professor of Computer Engineering at in the Department of Electrical and Computer Engineering at Iowa State University. He received his Ph.D degree in Computer Science and Engineering from the Indian Institute of Technology (IIT) and has been on the faculty of Iowa State University since 1999. His research expertise is in the areas of cyber-physical system (CPS) security for the smart grid, real-time systems & networks, and Internet of Things (IoT). He has co-authored 150 peer-reviewed research publications, and has given several invited talks and tutorials at reputed IEEE conferences, and delivered more than dozen industry short courses on the subject of cyber security for the power grid. He served as a guest co-editor for flagship IEEE publications (IEEE Network, IEEE Power & Energy), and serving as an Editor for IEEE Transactions on Smart Grid since 2013. He is the founding chair of the Cyber Security Task Force at IEEE PES and also currently serving as the Chair of the Computing and Analytical Methods for Power Systems (CAMS) Subcommittee. He is a co-author of the text "Resource Management in Real-time Systems and Networks," MIT Press, 2001.

Dr. Lalitha Sankar, Arizona State University

Lalitha Sankar received the B.Tech degree from the Indian Institute of Technology, Bombay, the M.S. degree from the University of Maryland, and the Ph.D degree from Rutgers University. She is presently an Assistant Professor in the ECEE department at Arizona State University. Prior to this, she was an Associate Research Scholar at Princeton University. Her research is focused on information privacy and cyber-security in distributed and cyber-physical systems. She received the NSF CAREER award in 2014. She received the IEEE Globecom 2011 Best Paper Award for her work on privacy of side-information in multi-user data systems. For her doctoral work, she received the 2007-2008 Electrical Engineering Academic Achievement Award from Rutgers University.

Dr. Sandip Roy, Washington State University

Sandip Roy is Professor and Associate Director of the School of Electrical Engineering and Computer Science at Washington State University. His research is primarily focused on developing techniques for estimation and control in dynamical networks, and using these techniques to enable secure and resilient operation of large-scale infrastructure networks including electric power and air transportation networks. Recently, he has also been involved in network analysis and design problems that arise in neurological and epidemiological processes. These research efforts have led to new models and algorithms, as well as software deployments, which are described in archival journal publications (about 60 in total) and conference articles (about 110 in total).

Dr. Gernot Heiser, Data61, CSIRO

Gernot Heiser is Scientia Professor and John Lions Chair of Operating Systems at UNSW Australia and Chief Research Scientist at Data61, CSIRO. He has a 20-year track record of building high-performance operating-system microkernels as a minimal basis for trustworthy systems. He is the founder and past leader of Data61's Trustworthy Systems group, which pioneered large-scale formal verification of systems code, specifically the design, implementation and verification of the seL4 microkernel. His former company Open Kernel Labs, acquired by General Dynamics in 2012, marketed the OKL4 microkernel, which shipped on billions of mobile wireless chips and more recently ships on the secure enclave processor of all iOS devices. Heiser is a Fellow of the ACM, the IEEE and the Australian Academy of Technology and Engineering (ATSE).

Kennan Skelly, Circadence

Ms. Skelly has more than fifteen years' experience in providing security and management solutions across a wide array of platforms to include personnel, physical, and cyber security. Ms. Skelly served in the US Army as an Explosive Ordnance Disposal Technician and went on to work for the Department of Homeland Security where she served as Chief for Comprehensive Reviews in the Assessments Branch of the Office for Infrastructure Protection. In this capacity she ran vulnerability assessments and exercises on Critical Infrastructure assets throughout the Nation, and helped to develop the first systems assessment approach for Critical Infrastructure and Key Resources. Ms. Skelly currently serves as Director, Strategic Marketing and Partnerships with Circadence Corporation. Ms. Skelly holds a B.A. in Homeland Security, a B.S. in Information Technology, a Masters Certificate in National Security Studies, and she is currently completing an M.P.S in Strategic Cyber Operations and Information Management at George Washington University.

Dr. Atul Prakash, University of Michigan

Atul Prakash is a Professor in Computer Science and Engineering at the University of Michigan with research interests in computer security and privacy. He received a Bachelor of Technology in Electrical Engineering from IIT, Delhi, India and a Ph.D. in Computer Science from the University of California, Berkeley. His current research is focusing on security of Internet of Things. His recent work on security analysis of the SmartThings cloud platform for hosting IoT apps received a Distinguished Practical Paper Award at IEEE Security and Privacy and also attracted press. His group has also recently developed a software framework, FlowFence, for enforcing information flow policies in IoT and mobile software.

Dr. Christopher Williams, Virginia Tech

Christopher B. Williams is the Electro-Mechanical Corporation Senior Faculty Fellow and an Associate Professor in the Department of Mechanical Engineering at Virginia Tech. He is the Director of the Design, Research, and Education for Additive Manufacturing Systems (DREAMS) Laboratory and Associate Director of the Macromolecules Innovation Institute (MII). His research contributions have been recognized by eight Best Paper awards at international design, manufacturing, and engineering education conferences. He is a recipient of a National Science Foundation CAREER Award (2013), the 2012 International Outstanding Young Researcher in Freeform and Additive Fabrication Award, and the 2010 Emerald Engineering Additive Manufacturing Outstanding Doctoral Research Award. Chris holds a Ph.D. and M.S. in Mechanical Engineering from the Georgia Institute of Technology (Atlanta, Georgia) and a B.S. with High Honors in Mechanical Engineering from the University of Florida (Gainesville, Florida).

Dr. John Hatcliff, Kansas State University

Dr. John Hatcliff is a University Distinguished Professor and Lucas-Rathbone Professor of Engineering at Kansas State University working in the areas of safety-critical systems, interoperable medical systems, software architectures, and software verification and certification. He leads the Laboratory on Static Analysis and Transformation of Software (SAnToS Lab), which has received funding from a number of national funding agencies and companies including Department of Defense, National Science Foundation, DARPA, Department of Homeland Security, NASA, NIH, Air Force Office of Scientific Research, Rockwell Collins, and Lockheed Martin. Dr. Hatcliff co-chairs the Architecture Requirements Working Group of the AAMI / UL 2800 Joint Committee that is developing safety standards for medical device interoperability. He has been an active member of the Medical Device Interoperability Safety Working Group that is currently interacting with the FDA on interoperability safety principles under the IDE program, and he collaborates closely with FDA engineers as part of the NSF FDA Scholar-in-residence program. In 2014 and 2015, he co-chaired the DoD-sponsored High Confidence Software and Systems conference.

Special Speakers and Attendees

Dr. Robert H. Bishop, University of South Florida

Dr. Robert H. Bishop is the Dean of Engineering at the University of South Florida and is a full professor in the Department of Electrical Engineering. He is a specialist in the area of systems and control theory. His current research interests are in the area of advanced navigation algorithm development with fast-to-flight characteristics, integrated navigation and guidance for planetary precision landing, small satellites and unmanned aerial vehicles. He co-authors one of the world's leading textbooks in control theory, and has authored two other textbooks, edited two handbooks, and authored/co-authored over one hundred and thirty-five journal and conference papers. Dr. Bishop is a Fellow of the American Institute of Aeronautics and Astronautics (AIAA) and a Fellow of the American Astronautical Association (AAS).

Dr. Sudeep Sarkar, University of South Florida

Dr. Sudeep Sarkar is Chair and professor of the Department of Computer Science and Engineering at the University of South Florida in Tampa. He received his M.S. and Ph.D. degrees in Electrical Engineering, on a University Presidential Fellowship, from The Ohio State University. He is the recipient of the National Science Foundation CAREER award in 1994, the USF Teaching Incentive Program Award for Undergraduate Teaching Excellence in 1997, the Outstanding Undergraduate Teaching Award in 1998, and the Theodore and Venette Askounes-Ashford Distinguished Scholar Award in 2004. He is a Fellow of the American Association for the Advancement of Science (AAAS), Institute of Electrical and Electronics Engineers (IEEE), American Institute for Medical and Biological Engineering (AIMBE), and International Association for Pattern Recognition (IAPR); and a charter member and member of the Board of Directors of the National Academy of Inventors (NAI). He has 25 year expertise in computer vision and pattern recognition algorithms and systems, holds three U.S. patents and has published high-impact journal and conference papers.

PI Demo Descriptions

Iowa State University:

PowerCyber is a hardware-in-the-loop CPS security testbed for smart grid developed at Iowa State University through a joint funding by the NSF and DHS via the NSF CPS program. The test-bed provides a realistic hybrid environment with a combination of simulated, emulated, and real components that capture cyber, control, and physical interactions. The primary domain of the testbed is the bulk power grid with emphasis on wide-area monitoring, protection, control (WAMPAC), and distributed decision. The testbed is currently being utilized for five main purposes: (i) *vulnerability analysis* in the SCADA environment, (ii) *impact analysis* due to successful cyber attacks including coordinated cyber attacks, (iii) cyber *attack-defense evaluations* to evaluate the effectiveness of the security and defense measures, (iv) university education and industry training on SCADA/ICS security, and (v) making the testbed broadly available to academic and industry community for security experimentations. This demo will showcase the integrated front-end and back-end environment of the testbed for experimentation via remote access. In addition, a couple of case study security experiments will be demonstrated, including an attack-defense demo on wide-area protection scheme of the power grid. The testbed has recently been utilized by several institutions for research and educational uses that include Symantec, Accenture, Applied Physics Lab @ John Hopkins University, PNNL, and University of Minnesota at Duluth.

NYU:

Software update systems for automobiles promise huge benefits at the cost of potential security vulnerabilities. No existing solution considers more advanced security objectives such as resilience against a repository compromise, selective blocking of update traffic by a MITM, or compromise at a supplier's site. To address this, we designed Uptane, a software update framework for automobiles that counters a comprehensive array of security attacks and that is resilient to partial compromises. Uptane address automotive specific vulnerabilities and limitations. Uptane is flexible and easy to adopt for industry stakeholders. Design details were developed together with the main automotive industry stakeholders in the USA. In this demonstration, we will show various attack scenarios and show how the attacks are prevented by Uptane.

HRL/UC Irvine:

Demonstrate a prototype of a seL4-enabled secure remote attestation (RA) on a commercial Sabre Lite development board. This is the first RA scheme to leverage a formally verified microkernel and requires minimal hardware assumptions. Although, the Sabre Lite board lacks secure boot support, we assume that seL4 boots first and immediately executes the special RA process which emulates the functionality of SMART architecture [1,2]. Other (one or more) application processes are then started. Upon request from the remote trusted verifier (running on a laptop-class device) the attestation process will compute and return an authenticated integrity check of the target application process. The verifier will thus determine whether the application process has been infected by malware.

Virginia Tech/Vanderbilt University:

While the digital thread of advanced manufacturing technologies is paving the way for a 4th Industrial Revolution ("Industry 4.0"), it is compromised by numerous cyber-physical vulnerabilities. In this demo, the team demonstrates unique cyber-physical vulnerabilities in additive manufacturing that can have significant impact on the printed part quality, and on the manufacturer's intellectual property. A web-based tool for modeling cyber-physical vulnerabilities within advanced manufacturing processes is also demonstrated. From these modeling tools, it is shown that alternative quality detection techniques are needed to determine if a part has potentially been compromised. Novel side-channel detection techniques, which employ vibration sensors to perform modal analysis on machined and 3D Printed parts, are demonstrated to successfully identify attacks on parts' internal and external structure.

Arizona State University:

The distributed electric power cyber-physical system is monitored and controlled by a cyber layer of networked intelligent devices and decision making centers that is essential for real-time situational awareness of the physical network. However, as with any cyber system, the electric CPS is susceptible to a variety of intelligent and sophisticated attacks including data integrity attacks. In our demo, we will highlight a class of data integrity attacks that allow an attacker with access to meters and data in only a sub-network to cause a line overload of a congested line such that the overload cannot be observed from the cyber system. The demo will highlight how an attacker with limited information can successfully evade the intelligent algorithms in the energy management systems and physically overload a line.

University of South Florida/Kansas State University/Honeywell:

In this demo, we carry out a cyber-attack in a mini building automation system (BAS). The attack is attempted at three BASs implemented using different operating systems as the controller platform: Linux, a security-enhanced MINIX, and seL4. We show that the attack can easily compromise the BAS's physical safety in the Linux-based system, but will be foiled in the security enhanced microkernel-based operating systems -- MINIX and seL4.

Adventium Labs:

Adventium will demonstrate several key components of the ISOSCELES results, including educational material, model based systems engineering, and a software prototype of our example patient-controlled analgesic pump.

Circadence:

Project Ares provides cyber security teams with a real-time opportunity to practice skills and hone tactics via a training platform designed to appeal to the learning style of the next generation. Project Ares deploys realistic, mission-specific virtual environments with actual cyber offense/defense tools, background network activity and a library of mission scenarios, available 24/7. Artificial intelligence components provide on demand support and feedback to players and greatly reduce the workload of instructors through automated scoring and dynamic opponents. To keep its content relevant, Project Ares employs a modular architecture that enables the platform to quickly and easily add new missions to address rapidly changing threats, tactics and tools. This level of agility in cyber training is unprecedented and necessary to keep up to date with the rapid evolution in cyber.

BYU/Washington State:

The mission-impact situational awareness tool will be demonstrated, in the context of a threat assessment of a water-management system on the Sevier River in Utah. The demonstration will focus on: 1) model and threat-scenario ingestion by the user, 2) automatic vulnerability and mission-impact analysis, and 3) counter-factual analysis. The demonstration will show how holistic impacts of threats arising from the human, cyber, and physical elements of this system can be assessed in a common framework. Ongoing work toward a second application testbed on air traffic management, and the investigators' communications with potential customers about the tool, will be briefly described.

MDISS:

The Medical Device Risk Assessment Platform (MDRAP) delivers a suite of services that provide health systems, key components of our nation's healthcare critical infrastructure, the ability to risk assess their medical devices to optimize patient and population safety. MDRAP supports the assessment of single devices and is architected to support aggregate risk for populations of devices and environmental adjustments for architecture. The risk assessment methodology is audit-based with questions derived from standards and best practices. Adoption and impact of MDRAP are amplified by the delivery of ancillary services that include inventory management, unique device identification, and crowdsourcing for efficiency and quality. Additional threat data feeds will be integrated into future releases.