Layered Assurance Workshop

PROGRAM

11th Layered Assurance Workshop

December 4-5, 2017

Orlando, Florida

Affiliated workshop of the
Annual Computer Security Applications Conference (ACSAC)

Monday, December 4th 2017

7:30-8:30	BREAKFAST
8:30-8:35	**Welcome and Opening Remarks** – Gabriela F. Ciocarlie and Peter G. Neumann
8:35-12:00	**Tutorial: *Holistic Layered Assurance*** Wolfgang Kampichler, Frequentis, Vienna, AT Topics covered: • Voice and data communication in air traffic management (as evaluation use case) • Layered assurance approach based on a communication demonstrator • Declarative language (MILS-AADL) for modeling distributed systems • Verification tools to prove security and dependability properties of a model • D-MILS Platform components (SK, MILS Console, MILS Network) • Tools to automate the development of an assurance case and to generate configurations for platform components • Use case deployment and evaluation results (practical examples)
12:00-13:30	LUNCH
13:30-14:15	**Invited Talk: *Fundamental Principles for Compositional Trustworthiness, and Their Relevance to the CHERI System Architecture*** Peter G. Neumann, SRI International, US We consider an extensive set of principles for the design, implementation, and operation of systems with critical trustworthiness requirements such as total-system security, reliability, and human safety. We also consider how these principles are foundational in the CHERI hardware-software architecture. However, by themselves they are not enough, as noted by C. Michael Holloway.
14:15-15:00	**Invited Talk: *Lawless: A skeptic's view of layered assurance*** Michael Holloway, NASA Langley Research Center, Hampton VA, US Safety assurance by composition of arguments is assuredly theoretically unsound. Theoretical unsoundness, however, does not necessarily imply practical impossibility, but it probably does. This talk will explore why.
15:00-15:30	BREAK
15:30-17:00	**Panel: *Reflections on the Future of Trustworthy Systems*** **Moderator**: Peter Neumann, SRI International, US This panel will consider implications from past efforts on what must be done in future research and development to achieve meaningfully trustworthy systems.

Tuesday, December 5th 2017

7:30-8:30	BREAKFAST
8:30-8:35	**Day 2 Opening Remarks**
8:35-12:00	**Tutorial: *Practical Formal Methods for the Analysis of Executable Code*** Sébastien Bardin, CEA LIST, FR Topics covered: • The benefits & challenges offered by binary code analysis • New challenges brought to formal methods by binary code analysis • Promising state-of-the-art techniques (Symbolic Execution, Abstract Interpretation) together with illustrating examples and discussions on limitations – including implementation issues and traps • Early achievements obtained by mitigating these limitations through well-chosen combinations of techniques
12:00-13:30	LUNCH
13:30-14:15	**Invited Talk: *Protecting Analog Sensor Security - OR - Sending Mixed Signals on IoT Cybersecurity*** Kevin Fu, University of Michigan, US Why are undergraduates taught to hold the digital abstraction as sacrosanct and unquestionable? Why do microprocessors blindly trust input from sensors, and what can be done to establish trust in unusual input channels in cyberphysical systems? Risks of analog sensor cybersecurity pose safety and security challenges to autonomous vehicles, medical devices, and the Internet of Things. Analog cybersecurity can also reduce risks by detecting an adversary via the physics of computation. Analog cybersecurity builds upon classic research in fault injection and side channels. This talk will highlight the risks of intentional RF, audible, and ultrasonic interference to integrity and availability of sensors. I will explain how to rethink the computing stack from electrons to bits to design out security risks that bubble up from physics into the operating system. This work brings some closure to my curiosity on why my cordless phone would ring whenever I executed certain memory operations on the video graphics chip of an Apple IIGS.
14:15-15:00	**Invited Talk: *Security Measures and Measurements for the Emerging Internet of Things*** Ulf Lindqvist, SRI International, Menlo Park, US The Internet of Things (IoT), where all kinds of devices – from public infrastructure to wearables – are being equipped with "smarts" and are being wirelessly connected, holds great promise to improve health, safety, and productivity in our society. However, the success of IoT is directly dependent on our ability to provide the right level of security, because the potential consequences of successful attacks could impact human lives and safety and cause death and destruction, directly or indirectly. We need new methods to automatically and continuously assess the level of security of IoT systems and networks, because if we cannot tell how changes to configurations or devices impact overall security, how will we be able to improve security with any degree of confidence? Also, we need to be able to design and select the most effective

	security mechanisms for large numbers of heterogeneous and often resource-limited IoT devices. This talk describes such challenges and opportunities, based on results from research conducted in the IoT Security and Privacy Center at SRI International.
15:00-15:30	BREAK
15:30-16:15	**Invited Talk:** ***Money For Nothing: Addressing Systemic Problems in Payment Systems*** Patrick G. Traynor, University of Florida, US Electronic payments come in a wide variety of embodiments, but one thing seems to pervade them all - widespread vulnerabilities. This talk covers weaknesses in emerging payment systems, as well as a discussion of the challenges of upgrading currently deployed infrastructure to more secure alternatives.
16:15-16:45	**Open Discussion:** ***Challenges in a Fully Automated IoT World*** **Moderator**: Gabriela Ciocarlie, SRI International, US
16:45-17:00	**The Future of LAW**
18:00-20:00	**ACSAC/LAW Reception**