Keynote 1:
Why Is It So Hard to Make Secure Chips?

Marc Witteman

Chief Executive Officer
Riscure

Chip security has long been the domain of smart cards. These microcontrollers are specifically designed to thwart many different attacks in order to deliver typical security functions as payment cards, electronic passports, and access cards.

With the advent of IoT everything is changing. Billions of devices will need security. We need access to our information sources and property. We expect our privacy to be respected and rely on the confidentiality of our sensitive information. We trust that our assets are well protected and cannot be manipulated by criminals. Can chip technology actually deliver on these demands?

In this presentation we start by looking at the security architecture of electronic devices and mechanisms to restrict access and protect information. Then we explain the threat landscape and explain different types of attacks. Next we zoom in to security properties of the chips, which are at the core of all electronic devices. Finally we show how attack resistance can be tested and how chip vendors can gain assurance about the security of their products.

Speaker's Bio:

Marc Witteman has a long track record in the security industry. He has been involved with a variety of security projects for over two decades and worked on applications in mobile communications, payment industry, identification, and pay television. Recent work includes secure programming and mobile payment security issues.

He has authored several articles on smart card and embedded device security issues. Further, he has extensive experience as a trainer, lecturing security topics for audiences ranging from novices to experts.

As a security analyst he developed several tools for testing software and hardware security. This includes Inspector, a platform for conducting side-channel analysis and JCworkBench, a logical test tool.

Marc Witteman has an MSc in Electrical Engineering from the Delft University of Technology in the Netherlands. From 1989 till 2001 he worked for several telecom operators, the ETSI standardization body and a security evaluation facility.

In 2001 he founded Riscure, a security lab based in the Netherlands. Riscure offers test tools and services to manufacturers and issuers of advanced security technology.

Between 2001 and 2009 he raised the company to a leading security test lab, and side channel test tool vendor. In 2010 Marc Witteman started Riscure Inc, the US branch of Riscure, based in San Francisco. At present he is the Chief Executive Officer of Riscure.

Keynote 2:

VLSI Design Methods for Low Power Embedded Encryption

Ingrid Verbauwhede

COSIC, KU Leuven and UCLA
www.esat.kuleuven.be/cosic

Intelligent things, medical devices, vehicles and factories, all part of cyberphysical systems, will only be secure if we can build devices that can perform the mathematically demanding cryptographic operations in an efficient way. Unfortunately, many of devices operate under extremely limited power, energy and area constraints. Yet we expect that they can execute, often in real-time, the symmetric key, public key and/or hash functions needed for the application. At the same time, we request that the implementations are also secure against a wide range of physical attacks.

This presentation will focus on the design methods to realize cryptographic operations on resource constrained devices. To reach the extremely low power, low energy and area budgets, we need to consider in an integrated way the protocols, the algorithms, the architectures and the circuit aspects of the application. These concepts will be illustrated with the design of several cryptographic co-processors suitable for implementation in embedded context.

Speaker's Bio:

Dr. Ingrid Verbauwhede is a Professor in the research group COSIC of the Electrical Engineering Department of the KU Leuven in Belgium. At COSIC, she leads the embedded systems and hardware group. She is also adjunct professor at the EE department at UCLA, Los Angeles, CA. She joined COSIC in 2003 and UCLA in 1998. Before joining UCLA she worked at UC Berkeley as a post-doctoral researcher and visiting lecturer, and later at TCSI and Atmel Lab in Berkeley, CA. She is a Member of IACR and a fellow of IEEE. She was elected as member of the Royal Flemish Academy of Belgium for Science and the Arts in 2011.

She is a pioneer in the field of efficient and secure implementations of cryptographic algorithms in embedded context on ASIC, FPGA and embedded SW. It has been the main focus of her PhD and of her research at UCLA and KU Leuven. At COSIC she also supervises the hardware electronics lab to perform side-channel and fault-attacks.

She is the author and co-author of more than 300 publications at conferences, journals, book chapters and books. She graduated 27 PhD students between 2004 and 2015, which have positions in academia and in industry, all over the world.

Dr. Verbauwhede has been the general chair in 2012 and the program chair in 2007 of the IACR CHES (Cryptographic Hardware and Embedded Systems) workshop, which is the flagship venue for secure hardware design. She has been member of the program committee of a large number of conferences, including DAC, DATE, ISSCC, Usenix, SIPS, ISCAS, ISLPED, and more.

Prof. Verbauwhede has participated in several EU funded hardware and embedded systems security projects. Currently her research group participates in the H2020 projects HECTOR and ECRYPT-CSA. Her list of publications and patents is available at www.esat.kuleuven.be/cosic.

Keynote 3:
Medical Device Security: The First 165 Years

Kevin Fu

University of Michigan

Today, it would be difficult to find medical device technology that does not critically depend on computer software. Network connectivity and wireless communication has transformed the delivery of patient care. The technology often enables patients to lead more normal and healthy lives. However, medical devices that rely on software (e.g., drug infusion pumps, linear accelerators, pacemakers) also inherit the pesky cybersecurity risks endemic to computing. What's special about medical devices and cybersecurity? What's hype and what's real? What can history teach us? How are international standards bodies and regulatory cybersecurity requirements changing the global manufacture of medical devices? This talk will provide a glimpse into the risks, benefits, and regulatory issues for medical device cybersecurity and innovation of trustworthy medical device software.

Speaker's Bio:

Kevin Fu is credited for establishing the field of medical device security beginning with the 2008 IEEE paper on defibrillator security. Kevin is Chief Scientist of Virta Labs, Inc. and Associate Professor in EECS at the University of Michigan where he directs the Archimedes Center for Medical Device Security and the Security and Privacy Research Group (SPQR).

Kevin has testified in the House and Senate on matters of information security and has written commissioned work on trustworthy medical device software for the Institute of Medicine of the National Academies. He is member of NIST Information Security and Privacy Advisory Board, the CRA Computing Community Consortium Council, and the ACM Committee on Computers and Public Policy. He was named MIT Technology Review TR35 Innovator of the Year. Kevin served as program chair of USENIX Security during a period of unprecedented growth. He co-chairs the AAMI Working Group on Medical Device Security. He served as a visiting scientist at the Food & Drug Administration, the Beth Israel Deaconess Medical Center of Harvard Medical School, Microsoft Research, and MIT CSAIL. Fu received his B.S., M.Eng., and Ph.D. from MIT. He earned a certificate of artisanal bread making from the French Culinary Institute.

Keynote 4:

Design and Implementation of
Real-Time Multi-sensor Vision Systems

Yusuf Leblebici

Swiss Federal Institute of Technology, Lausanne (EPFL)

Implementation of high performance multi-camera / multi-sensor imaging systems that are required to produce real-time video output pose a large number of unique challenges to conventional digital design based on general-purpose processors or GPUs. In potential application areas ranging from machine vision, automotive, and virtual reality, the need for real-time operation with very limited latency dictates customized architectures that are not readily implementable using conventional approaches. In this talk, we will discuss the algorithms that are utilized in such multi-sensor platforms, the specialized architectures that allow streaming video processing, and system-level integration issues. Problems such as light-field reconstruction, multi-band blending, pixel-level interpolation, and rectification are presented, with detailed circuit and system level examples.

Speaker's Bio:

Yusuf Leblebici received the B.Sc. and M.Sc. degrees in electrical engineering from Istanbul Technical University, Istanbul, Turkey, in 1984 and 1986, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Illinois, Urbana-Champaign (UIUC), in 1990. Since 2002, he is a Chair Professor at the Swiss Federal Institute of Technology in Lausanne (EPFL), and director of Microelectronic Systems Laboratory. His research interests include design of high-speed CMOS digital and mixed-signal integrated circuits, computer-aided design of VLSI systems, intelligent sensor interfaces, modeling and simulation of semiconductor devices, and VLSI reliability analysis. He is the coauthor of six textbooks, as well as more than 300 articles published in various journals and conferences. He is a Fellow of IEEE since 2010, and he has been elected as Distinguished Lecturer of the IEEE Circuits and Systems Society for 2010-2011.