



Association for
Computing Machinery

Advancing Computing as a Science & Profession

NEWS RELEASE

CONTACT: Jim Ormond
212-626-0505
ormond@hq.acm.org

WORLD'S LEADING CYBERSECURITY RESEARCHERS TO CONVENE IN VIENNA

*Major ACM Conference Examines Security in Areas Including Mobile Devices,
Power Grids and Transportation Systems*

New York, NY, October 12, 2016 – The recent announcement by Yahoo! that hackers may have stolen data from up to 500 million user accounts is just the latest disclosure of a major data breach, and begs the question, “Are we keeping ahead or falling behind in our efforts to keep our computers and devices secure?” The Association for Computing Machinery’s Special Interest Group on Security, Audit and Control (SIGSAC) will hold its 23rd annual conference on Computer and Communications Security (CCS) from October 24 – 28 in Vienna, Austria. The conference brings together information security researchers, practitioners, developers, and users from all over the world to explore cutting-edge ideas and results. From its inception, CCS established itself as a high-standard research conference in the computer security area.

The main conference program is organized around five main tracks: Cryptographic Mechanisms; Differential Privacy/Cryptography Attacks, Web/Mobile Security, Secure Code and Systems, and Tutorials and Invited Talks. Rounding out the program are planned keynote addresses, workshops, and a presentation of research posters.

“CCS is our flagship annual conference and we are especially proud of the program we have put together this year,” said General Conference Co-Chair Edgar Weippl, SBA Research. “We have planned presentations on everything from the security of cyber-physical systems to smart phones and blockchains. Professionals in the computer and communications security field especially benefit by coming together and sharing the challenges they have faced and how they have overcome them.”

Organizers expect attendees drawn from both academia and industry. “As always, our attendees recognize CCS as a venue where new research is presented,” added General Conference Co-Chair Stefan Katzenbeisser, TU Darmstadt, CYSEC. “This year we have more than 850 people from 40 countries registered for CCS—an attendance record for the conference. Also new this year, CCS will include a special three-part program on crypto currencies.”

CCS 2016 Highlights Include:

Keynote Addresses

Martin Hellman, “Cybersecurity, Nuclear Security, Alan Turing, and Illogical Logic”

Hellman is best known for his invention, with Whitfield Diffie and Ralph Merkle, of public key

cryptography, the technology that, among other uses, enables secure Internet transactions. Hellman and Diffie received the 2015 ACM A.M. Turing Award for work in this area. Hellman has a deep interest in the ethics of technological development. One of his current activities is applying risk analysis to a potential failure of nuclear deterrence.

Ross Anderson, “Is It Practical to Build a Truly Distributed Payment System?”

Anderson is one of the founders of the economics of information security, a growing new academic discipline. He will discuss the latest technologies that make payment transactions faster, more resilient and more secure.

New Three-Part Program on Crypto Currencies

(Part 1) *Aljoshia Judmayer, “Crypto Currencies Crash Course”*

This tutorial aims to close the gap between IT security research and the area of cryptographic currencies and blockchains. Bitcoin, the most prominent cryptocurrency, will be used as an example to discuss underlying blockchain mechanics.

(Part 2) *Aniket Kate, “Introduction to Credit Networks”*

This tutorial first defines the concept of IOU credit networks, and then describes some of the important credit network applications. The presenter will then describe and analyze recent and ongoing projects to improve the credit-network security, privacy and reliability.

(Part 3) *Ghassan O. Karame, “On the Security and Scalability of Bitcoin’s Blockchain”*

This tutorial provides an overview, detail, and analysis of the security provisions of Bitcoin and its underlying blockchain—effectively capturing recently reported attacks and threats in the system. The presentation will go beyond the mere analysis of reported vulnerabilities of Bitcoin; namely, it will describe and evaluate a number of countermeasures to deter threats on the system, some of which have already been incorporated in the system.

Invited Industry Talks

Timo Kasper, “Colorful Like a Chameleon: Security Nightmares of Embedded Systems”

A combination of side-channel attacks, reverse-engineering and mathematical cryptanalysis helps to reveal and exploit weaknesses in the systems that, for example, allow opening secured doors in seconds. The use of open-source project ChameleonMini is presented as a possible tool in the fight against these kinds of attacks.

Thorsten Bormann, “Design Requirements on Resilient Command Control and Signaling Systems in the Railway Sector—First Preliminary Results of the CYSIS Working Group on IT Security”

Bormann, whose company oversees approval management for railway control command and signaling systems in Germany, will discuss approaches to cybersecurity for critical transportation infrastructures.

Klaus Kursawe, “Experiences in Securing Smart Grids and their Operations”

The electricity distribution grid is one of the most complex and critical systems built by mankind. This system is currently in a process of massive digitalization. The corresponding security needs are a challenge for grid operators and their suppliers, where numerous vulnerabilities have recently emerged in smart grid architectures, protocols, and device implementations.

Selected Papers

- “A Secure Sharding Protocol for Open Blockchains”
- “Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition”
- “Acing the IOC Game: Toward Automatic Discovery and Analysis of Open-Source Cyber Threat Intelligence”
- “Error Handling of In-vehicle Networks Makes Them Vulnerable”
- “Generic Attacks on Secure Outsourced Databases”
- “iLock: Immediate and Automatic Locking of Mobile Devices against Data Theft”
- “Leave Your Phone at the Door: Side Channels that Reveal Factory Floor Secrets”
- “My Smartphone Knows What You Print: Exploring Smartphone-based Side-channel Attacks Against 3D Printer”
- “On the Instability of Bitcoin without the Block Reward”
- “SmartWalk: Enhancing Social Network Security via Adaptive Random Walks”

For a full conference program, please visit [CCS2016](#).

About ACM SIGSAC

The ACM Special Interest Group on Security, Audit and Control's (<https://www.sigsac.org/>) mission is to develop the information security profession by sponsoring high quality research conferences and workshops. SIGSAC conferences address all aspects of information and system security, encompassing security technologies, secure systems, security applications, and security policies.

About ACM

ACM, the Association for Computing Machinery (www.acm.org), is the world's largest educational and scientific computing society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

###