# CCS 2016 Conference Organization

| General co-Chairs: | Edgar Weippl  
(SBA Research, Austria) |  
Stefan Katzenbeisser  
(TU Darmstadt, CYSEC, Germany) |
|-------------------|-------------------|-------------------|
| Program co-Chairs: | Christopher Kruegel  
(University of California, Santa Barbara, USA) |  
Andrew Myers  
(Cornell University, USA) |
| Workshop co-Chairs: | Mathias Payer  
(Purdue University, USA) |  
Stefan Mangard  
(IAIK TU Graz, Austria) |
| Tutorial co-Chairs: | Frederik Armknecht  
(University Mannheim, Germany) |  
Gregory Neven  
(IBM Zurich Research Laboratory, Switzerland) |
| Poster/Demo co-Chairs: | Andreas Peter  
(University of Twente, The Netherlands) |  
Dominique Schröder  
(Saarland University, Germany) |
| Panel Chair: | Ahmad-Reza Sadeghi  
(TU Darmstadt, CYSEC, Germany) |
| Student Travel Grant co-Chairs: | Hassan Takabi  
(University of North Texas, USA) |  
Stefan Brunthaler  
(SBA Research, Austria) |
| Publicity co-Chairs: | Mauro Conti  
(University of Padua, Italy) |  
Anja Lehmann  
(IBM Research Zurich, Switzerland) |
| Sponsor/Industry Outreach: | Florian Kerschbaum  
(SAP, Germany) |
| Social Media Chair: | Martin Schmiedecker  
(SBA Research, Austria) |
| Proceedings Chair: | Stefan Katzenbeisser  
(TU Darmstadt, CYSEC, Germany) |
| Head of Organization: | Yvonne Poul  
(SBA Research, Austria) |
| Steering Committee Chair: | Somesh Jha  
(University of Wisconsin, Madison, US) |
| Steering Committee: | Helen Wang  
(Microsoft Research, USA) |
| | Carl Landwehr  
(University of Washington, USA) |
| | Giovanni Vigna  
(University of California, Santa Barbara, USA) |
| | George Danezis  
(University College London, UK) |
| | Trent Jaeger  
(SIGSAC Chair) |
| | Stefan Savage  
(University of California, San Diego, USA) |
| | David Basin  
(ETH Zurich, Switzerland) |
CCS 2016 General Chair's Welcome

It is our great pleasure to welcome you to the 2016 ACM Conference on Computer and Communications Security. CCS is the flagship annual conference of the Special Interest Group on Security, Audit, and Control (SIGSAC) of the Association for Computing Machinery. CCS brings together information security researchers, practitioners, developers, and users from all over the world to explore cutting-edge ideas and results. It provides an environment to conduct intellectual discussions. From its inception, CCS has established itself as a high standard research conference in its area. Its reputation continues to grow and is reflected in the prestigious technical program.

We are proud to say that CCS 2016 is the largest CCS conference ever. From 2002 to 2015, the number of submission rose from roughly 150 to 660. This year, CCS received the record number of 831 submissions. Together with 14 workshops, 7 tutorials, 3 invited industrial talks, a panel discussion and two prestigious keynote speeches by Martin Hellman and Ross Anderson, CCS 2016 probably is the largest scientific event in the area of information security. We are happy to welcome more than 900 participants from 40 countries. To give you the opportunity to exchange ideas with other researchers and practitioners in a relaxed atmosphere, we have organized two social events: a Mayor’s Dinner at the Vienna City Hall (Tuesday, Oct 25) and a traditional Viennese Dinner in a wine tavern (Wednesday, Oct 26).

CCS 2016 would not have been possible without the help of numerous volunteers. We first want to thank all authors who have submitted their work to CCS – without their commitment CCS 2016 would never have been possible. We furthermore want to thank the Program Committee, who diligently supported the peer review process and selected an interesting program. Finally, we want to thank the Program Chairs and the entire Organization and Steering Committee for their dedication and commitment. Special thanks go to Yvonne Poul and her team for the wonderful handling of the organization. Last but not least, we would like to express our gratitude to our generous sponsors.

We hope that you will find this program interesting and thought-provoking and that the conference will provide you with a valuable opportunity to share ideas with other researchers and practitioners from institutions around the world. We wish you a pleasant stay in Vienna – enjoy CCS 2016!

Stefan Katzenbeisser
CCS 2016 General co-Chair
TU Darmstadt, CYSEC, Germany

Edgar Weippl
CCS 2016 General co-Chair
SBA Research, Austria

Shai Halevi
CCS 2016 Program Co-Chair
IBM Research, USA

Christopher Kruegel
CCS 2016 Program Co-Chair
UC Santa Barbara, USA

Andrew Myers
CCS 2016 Program Co-Chair
Cornell University, USA

CCS 2016 Program Chair’s Welcome

It is our pleasure to present the proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS 2016), held in Vienna, Austria, on October 24 - 28, 2016. All papers in the proceedings were subject to a rigorous process of peer review. We received 831 fully reviewed submissions, the largest number of submissions received to date by a computer security conference. A Program Committee comprising 141 experts from 20 countries, helped by 360 external reviewers, evaluated these submissions, employing the customary double-blind review procedure. The review process had a 16.5% acceptance rate, resulting in 137 papers being accepted to the program, and very broad coverage of the entire security area.

The review process was organized in three phases. In the first review round, at least two preliminary reviews were written for each paper. Most papers went on to a second round, during which at least one additional review was solicited. At this point, the authors were given an opportunity to respond to the comments received (in a rebuttal phase). Finally, in the third round, the program committee actively and comprehensively discussed the papers, and, if necessary, requested additional reviews. Within the program committee, a “rebuttal committee” subgroup helped to spur discussion, to ensure that author responses were considered carefully, and to reflect the post-review discussion in the feedback to authors. New this year, we relied heavily on the TPMS system for assigning submissions to reviews, and we thank Laurent Charlin for writing this system and for all his help with using it.

We are profoundly grateful to the members of the Program Committee for their hard work, professionalism, and responsiveness under very tight deadline requirements. On average, PC members reviewed 17 papers. We are also indebted to the external reviewers whose focused expertise added substantial value to the feedback for authors. Moreover, we want to thank the CCS 2016 conference committee: the general chairs, workshop, poster, and tutorial co-chairs, and other chairs and organizers, as well as the steering committee, for their advice on how to produce a strong program and for their help with these proceedings. Finally, we thank the authors of all submitted papers and all attendees for their participation in the technical discussion during the conference. We hope that you find the program stimulating and helpful in advancing the exciting area of computer and communications security.

Edgar Weippl
CCS 2016 General co-Chair
IBM Research, USA

Shai Halevi
CCS 2016 Program Co-Chair
IBM Research, USA

Christopher Kruegel
CCS 2016 Program Co-Chair
UC Santa Barbara, USA

Andrew Myers
CCS 2016 Program Co-Chair
Cornell University, USA
Cybersecurity, Nuclear Security, Alan Turing, and Ilogical Logic

Abstract: My work that was recognized by the 2015 ACM Turing Award is in cybersecurity, while my primary interest for the last 35 years has been international security with an emphasis on reducing the risk that nuclear deterrence will fail and destroy civilization. This ACM Turing Lecture draws connections between those seemingly disparate areas and Alan Turing’s elegant proof that the computable real numbers, while denumerable, are not effectively denumerable.

Martin E. Hellman is best known for his invention, with Diffie and Merkle, of public key cryptography, the technology that, among other uses, enables secure Internet transactions. It is used to transfer literally trillions of dollars every day. He has been a long-time contributor to the computer privacy debate, and was a key participant in the “first crypto war” of the late 1970s and early 80s that established the right of academic cryptographic researchers to publish their papers, free of government interference.

His work has been recognized by a number of honors and awards, including election to the National Academy of Engineering, induction as an academic cryptographic researcher to publish his papers, free of government interference. His work has been recognized by a number of honors and awards, including election to the National Academy of Engineering, induction as an academic cryptographic researcher to publish his papers, free of government interference. His work has been recognized by a number of honors and awards, including election to the National Academy of Engineering, induction as an academic cryptographic researcher to publish his papers, free of government interference. His work has been recognized by a number of honors and awards, including election to the National Academy of Engineering, induction as an academic cryptographic researcher to publish his papers, free of government interference. His work has been recognized by a number of honors and awards, including election to the National Academy of Engineering, induction as an academic cryptographic researcher to publish his papers, free of government interference.

most recently, the 2015 ACM Turing Award, often called “the Nobel Prize of Computer Science.” More detailed information is available on his honors and awards, his university service, and his professional and civic service.

Hellman has a deep interest in the ethics of technological development, and one of his current activities is applying risk analysis to a potential failure of nuclear deterrence. That approach has been endorsed by a number of prominent individuals including former Director of the National Security Agency (NSA) Adm. Bobby Inman and Stanford’s President Emeritus Donald Kennedy.

Born in New York, NY in October 1945, he received his B.E. from New York University in 1966, and his M.S. and Ph.D. from Stanford University in 1967 and 1969, all in Electrical Engineering. Prof. Hellman was at IBM’s Watson Research Center from 1968-69 and an Assistant Professor of Electrical Engineering at MIT from 1969-71. Returning to Stanford in 1971, he served on the regular faculty until becoming Professor Emeritus in 1996. He has authored over seventy technical papers, twelve US patents and a number of foreign equivalents.

Is it practical to build a truly distributed payment system?

Abstract: Early payment systems were truly distributed; Alice gave Bob some precious metal or fancy printing. So were some early electronic systems, such as Mondex, which relied on value counters in tamper-resistant smartcards. But probably the only such mechanisms now fielded at scale are prepaid electricity meters (mostly using the STS specification, which the author helped develop in the 1990s).

Since then, the trend has been to centralise. First, ATMs went online only; second, we moved to EMV, which relies on shared-key crypto between the card and the card issuing bank; third, we got mobile money systems like M-Pesa that use encrypted SMS or USSD sessions with a central server; and most recently we have bitcoin, with its distributed implementation of a central server.

Yet about one sixth of humanity live in areas where the GSM network is flaky or absent. It’s bad enough to have to walk miles to use a mobile phone, but even worse if the village shop can’t accept mobile payments, which have been transformative in much of the developing world. As part of a financial inclusion project sponsored by the Gates Foundation, we have built and field-tested a prototype mobile payment system, DigiTally, for use offline. The crypto is simple enough: a challenge is copied from the payee’s phone to the payer’s, and an authorisation code is then copied back to the payee. Careful usability engineering makes DigiTally easier to use for both merchants and customers than a traditional phone payment system such as M-Pesa. It still works where there is no network, and can be cheaper where there is one.

This may have broader implications. Wherever we build delay-tolerant networks, we will need delay-tolerant authentication, and often delay-tolerant payments too. And as tamper-resistant devices proliferate – in SIM cards, TPM chips, NFC secure elements, and processors supporting mechanisms such as TrustZone and SGX – there may be many applications where they can make transactions faster and more resilient rather than just more secure.

Ross Anderson is Professor of Security Engineering at Cambridge University. He is one of the founders of a vigorously-growing new academic discipline, the economics of information security. Ross was also a seminal contributor to the idea of peer-to-peer systems and an inventor of the AES finalist encryption algorithm “Serpent”. He also wrote the standard textbook “Security Engineering – a Guide to Building Dependable Distributed Systems”.

Tuesday, October 25, 2016, 08.50-09.50, Lecture Hall C

Wednesday, October 26, 2016, 08.50-09.50, Lecture Hall C
Colorful like a Chameleon:
Security Nightmares of Embedded Systems

Abstract: Wireless embedded devices have become omnipresent in applications such as access control (to doors or to PCs), identification, and payments. The talk reviews the security of several commercial devices that typically employ cryptographic mechanisms as a protection against ill-intended usage or to prevent unauthorized access to secured data. 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. At hand of real-world examples and live demos, the implications of a key extraction for the security of the respective contactless application are illustrated. As a powerful tool for security-analyzing and pentesting NFC and RFID systems, the open-source project “ChameleonMini” is presented: Besides virtualization and emulation of contactless cards, the device allows to log the NFC communication, and in its latest revision acts as an active RFID reader to copy contactless cards on-the-fly.

Timo Kasper has studied electrical engineering and information technology at the Ruhr-University Bochum, Germany and at the University of Sheffield, UK. In 2006, his Diploma thesis “Embedded Security Analysis of RFID Devices” won the first place award for IT security (CAST, Darmstadt). He continued as a researcher at the Chair for Embedded Security of the Horst Görtz Institute for IT Security (HGI) and completed his studies 2011 with a PhD in Engineering. Since 2012, Timo has been co-founder and executive director of Kasper&Oswald GmbH, offering innovative products and services for security engineering.

Timo’s field of expertise covers the security of embedded cryptographic systems such as smartcards, microcontrollers, and FPGAs, with a focus on RFID and wireless applications. He is interested in security analyses and penetration testing, implementation attacks (side-channel analysis, fault injection), reverse engineering, and system-level viewpoints of security. He enjoys implementing cryptography on embedded systems and efficiently securing them with countermeasures. His publications demonstrate various security vulnerabilities of real-world applications, e.g., by breaking access control systems (KeeLoq – CRYPTO 2008, SimonsVoss – CRYPTO 2013), a payment system (Financial Crypto 2010), the security mechanism of widespread FPGAs (ACM CCS 2011) and remote keyless entry systems of cars (Usenix Security 2016).

Design requirements on resilient command control and signaling systems in the railway sector – first preliminary results of the CYSIS working group on IT security

Abstract: Managing of the railway infrastructure in Germany is performed by DB Netz AG. In order to be able to be still competitive in a constantly changing market for transport services, it is necessary to further improve the performance of the railway network and in parallel to reduce the life-cycle costs for the future systems. Currently, proprietary systems and closed communication infrastructures are in operation, for future system architectures commercial-off-the-shelf devices and common, i.e. open communication networks are intended to be used. Especially the safety-relevant control command and signaling systems, which have still reached a high level of functional safety, are in focus.

Deutsche Bahn AG and Technical University of Darmstadt (TU Darmstadt) have set up an innovation alliance to provide a platform for close collaboration and interdisciplinary research projects in the field of railway networks, mobility and logistics (DB RailLab). Within this platform the working group CYSIS (Cybersecurity for safety-relevant critical infrastructures) was founded in 2016 to meet the rising challenges for IT security in the railway sector. One current startup project is concerned with the development of requirements for resilient system architectures.

The speech mainly presents first preliminary results of the CYSIS working group from a best-practice perspective.

Thorsten Borrmann studied physics at Ruhr-University Bochum and began his career in the field of nuclear safety. Since 2015 he is working in the department for approval management for railway control command and signaling systems at DB Netz AG. He is responsible for the new German approval process for control command and signaling systems and is advisor for safety risk analyses, especially in relation to the European common safety methods for risk assessment. He is a member of the CYSIS working group for resilient architectures and has a deep interest in security for safety concepts.
Experiences in Securing Smart Grids and their Operations

Abstract: The power distribution grid is one of the most complex and critical systems built by mankind. This system is currently in a process of massive digitalization. This “smart grid” promises to improve the reliability and efficiency by introducing automated control systems on several levels of electricity distribution, and is a vital component of integrating renewable energy sources and electric vehicles. In a few years, the grid will be unable to operate without large-scale digital control systems.

The corresponding security needs are not only a challenge for grid operators and their suppliers, where numerous vulnerabilities have recently emerged in smart grid architectures, protocols, and implementations. The requirements imposed by the smart grid environment and constraints include a device lifetime of several decades, extremely limited communication abilities, and a vast geographical distribution. This often pushes security providers to their limits, and the classical IT approach can even be counterproductive. Furthermore, the different view of protecting a safety-critical physical process rather than information is an enduring source of conflict between operations and IT.

This talk summarizes the experiences of working with grid operators through trainings, attack simulations, device- and protocol testing, consulting, research and information-sharing activities. This covers the current state of smart grid security and privacy and discusses approaches and needs for smart grids on the design, operational and organizational level.

Klaus Kursawe received his PhD from the University of Saarbrücken in collaboration with IBM Research in 2001, working on secure dependable systems. From 2006 till 2010, he headed the “Trusted Systems Cluster” at Philips Natlab. There, he started working on security aspects and standards regarding the smart grid, which he continued after starting to teach at Radboud University. In 2012, he co-founded the European Network for Cybersecurity, an organization owned and funded by grid operators to assist them with security in smart grids, where he also worked as the Chief Scientist until 2016. In this context, he was member of several EU and US expert groups on smart grids, performed trainings for grid operators and other critical infrastructure owners, and was involved in risk analysis, procurement requirement design as well as both the security analysis and security design for smart grid protocols and components.

Program Anomaly Detection: Methodology and Practices

Abstract: This tutorial will present an overview of program anomaly detection, which analyzes normal program behaviors and discovers aberrant executions caused by attacks, misconfigurations, program bugs, and unusual usage patterns. It was first introduced as an analogy between intrusion detection for programs and the immune mechanism in biology. Advanced models have been developed in the last decade and comprehensive techniques have been adopted such as hidden Markov model and machine learning.

We will introduce the audience to the problem of program attacks and the anomaly detection approach against threats. We will give a general definition for program anomaly detection and derive model abstractions from the definition. The audience will be walked through the development of program anomaly detection methods from early-age n-gram approaches to complicated pushdown automata and probabilistic models. This procedure will help the audience understand the objectives and challenges in designing program anomaly detection models. We will discuss the attacks that subvert anomaly detection mechanisms. The field map of program anomaly detection will be presented. We will also briefly discuss the applications of program anomaly detection in Internet of Things security. We expect the audience to get an idea of unsolved challenges in the field and develop a sense of future program anomaly detection directions after attending the tutorial.

Xiaokui Shu is a Research Staff Member in the Security Services Team (GSAL) at the IBM Thomas J. Watson Research Center. He received his Ph.D. degree in computer science at Virginia Tech. His research interests are in system and network security, such as intrusion detection, data leak detection, and mobile security. He graduated from Virginia Tech with an Outstanding Ph.D. Student Award at the Department of Computer Science and graduated from the University of Science and Technology of China (USTC) with Guo Moruo Award as an undergraduate.

Danfeng (Daphne) Yao is an associate professor in the Department of Computer Science at Virginia Tech, Blacksburg. She is an Elizabeth and James E. Turner Jr. ’56 Faculty Fellow and L-3 Faculty Fellow. She received her Computer Science Ph.D. degree from Brown University in 2007. She received the NSF CAREER Award in 2010 for her work on human-behavior driven malware detection, and most recently ARO Young Investigator Award for her semantic reasoning for mission-oriented security work in 2014.

Wednesday, October 26, 2016, 17.15-18.00, Lecture Hall E

Tuesday, October 25, 2016, 10.00-11.30, Lecture Hall E - Tutorial 1
Security on Wheels: Security and Privacy for Vehicular Communication Systems

Abstract: This tutorial is concerned with the design of appropriate security and privacy mechanisms and their integration with VC functionality, especially in the light of strict requirements of VC-enabled safety applications. We consider architectural issues, a wide range of protocols, their analysis, and related implementation aspects. The focus will shift as needed: from an in-depth technical treatment to broader applicability and organizational matters; from the common understanding in industry and standardization bodies to future enhancements and developments, to the latest on implementation and field operational testing. We will first introduce the basics of VC systems and identify related vulnerabilities and threats. Then, we will outline requirements and present the state-of-the-art solution space. In brief, the following will be covered:

- System assumptions and enabling technologies, adversarial models, security and privacy requirements
- Basic concepts and architectures for secure and privacy enhancing VC systems
- Security mechanisms, facilities, and protocols
- Identity, key, and credential management
- In-car communication and platform security
- Secure and privacy-preserving VC protocols
- Vehicle-to-vehicle/vehicle-to-infrastructure

Panagiotis (Panos) Papadimitratos earned his Ph.D. degree from Cornell University, Ithaca, NY, in 2005. He then held positions at Virginia Tech, EPFL and Politecnico of Torino. Panos is currently a tenured Associate Professor at KTH, Stockholm, Sweden, where he leads the Networked Systems Security group. His research agenda includes a gamut of security and privacy problems, with emphasis on wireless networks. At KTH, he is affiliated with the ACCESS center, leading its Industrial Competence Group on Security. Panos is a Knut and Alice Wallenberg Academy Fellow and he received a Swedish Science Foundation Young Researcher Award.

Cryptographic Currencies Crash Course (C5)

Abstract: “Bitcoin is a rare case where practice seems to be ahead of theory.” Joseph Bonneau et al. [20]

This tutorial aims to further close the gap between IT security research and the area of cryptographic currencies and block chains. We will describe and refer to Bitcoin as an example throughout the tutorial, as it is the most prominent representative of a such a system. It also is a good reference to discuss the underlying block chain mechanics which are the foundation of various altcoins (e.g. Namecoin) and other derived systems.

In this tutorial, the topic of cryptographic currencies is solely addressed from a technical IT security point of view. Therefore we do not cover any legal, sociological, financial and economical aspects. The tutorial is designed for participants with a solid IT security background, but will not assume any prior knowledge on cryptographic currencies. Thus, we will quickly advance our discussion into core aspects of this field.

Panos Papadimitratos
KTH, Sweden

Aljosha Judmayer
SBA Research, Austria

Tuesday, October 25, 2016, 14.30-16.00 & 16.30-18.00, Lecture Hall E - Tutorial 2

Wednesday, October 26, 2016, 10.00-11.30, Lecture Hall E - Tutorial 3
Introduction to Credit Networks
(CCS)^2 – Crypto-Currencies Special @ CCS 2016

Abstract: Credit networks model transitive IOWeYou (IOU) credit between their users. With their flexible-yet-scalable design and robustness against intrusion, we are observing a rapid increase in their popularity as a backbone of real-world permission-less payment settlement networks (e.g., Ripple and Stellar) as well as several weak-identity systems requiring Sybil-tolerant communication. In payment scenarios, due to their unique capability to unite emerging crypto-currencies and user-defined currencies with the traditional fiat currency and banking systems, several existing and new payment enterprises are entering in this space. Nevertheless, this enthusiasm in the market significantly exceeds our understanding of security, privacy, and reliability of these inherently distributed systems. Currently employed ad hoc strategies have left those systems vulnerable to bigger problems once they become lucrative targets for malicious players.

In this tutorial, we first define the concept of IOU credit networks and describe some of the important credit network applications. We then describe and analyze recent and ongoing projects to improve the credit-network security, privacy and reliability. We end our discussion with interesting open problems and system challenges in the field. This introductory tutorial is accessible to the standard CCS audience with graduate-level security knowledge.

Aniket Kate is an assistant Professor in the the computer science department at Purdue university. He designs, implements, and analyzes privacy- and transparency-enhancing technologies for networked systems. His current research integrates cryptography, distributed computing, and trusted hardware. Before joining Purdue in 2015, Prof. Kate was a junior faculty member and an independent research group leader at Saarland University in Germany, where he was heading the Cryptographic Systems Research Group. He was a postdoctoral researcher at Max Planck Institute for Software Systems (MPI-SWS), Germany from 2010 until 2012, and he received his PhD from the University of Waterloo, Canada in 2010.

On the Security and Scalability of Bitcoin’s Blockchain
(CCS)^2 – Crypto-Currencies Special @ CCS 2016

Abstract: The blockchain emerges as an innovative tool which proves to be useful in a number of application scenarios. A number of large industrial players, such as IBM, Microsoft, Intel, and NEC, are currently investing in exploiting the blockchain in order to enrich their portfolio of products. A number of researchers and practitioners speculate that the blockchain technology can change the way we see a number of online applications today. Although it is still too early to tell for sure, it is expected that the blockchain will stimulate considerable changes to a large number of products and will positively impact the digital experience of many individuals around the globe.

In this tutorial, we overview, detail, and analyze the security provisions of Bitcoin and its underlying blockchain – effectively capturing recently reported attacks and threats in the system. Our contributions go beyond the mere analysis of reported vulnerabilities of Bitcoin; namely, we describe and evaluate a number of countermeasures to deter threats on the system, some of which have already been incorporated in the system. Recall that Bitcoin has been forked multiple times in order to ne-tune the consensus (i.e., the block generation time and the hash function), and the network parameters (e.g., the size of blocks). As such, the results reported in this tutorial are not only restricted to Bitcoin, but equally apply to a number of “altcoins” which are basically clones/forks of the Bitcoin source code. Given the increasing number of alternative blockchain proposals, this tutorial extracts the basic security lessons learnt from the Bitcoin system with the aim to foster better designs and analysis of next-generation secure blockchain currencies and technologies.

Ghassan O. Karame is a Senior Researcher in the Security Group of NEC Research Laboratories in Germany. Until April 2012, he was working as a postdoctoral researcher in the Institute of Information Security of ETH Zurich, Switzerland. He holds a Master of Science degree in Information Networking from Carnegie Mellon University (CMU), and a PhD degree in Computer Science from ETH Zurich. Ghassan is interested in all aspects of security and privacy with a focus on cloud security, SDN/network security, and Bitcoin security.
Privacy and Security in the Genomic Era

Abstract: With the help of rapidly developing technology, DNA sequencing is becoming less expensive. As a consequence, the research in genomics has gained speed in paving the way to personalized (genomic) medicine, and geneticists need large collections of human genomes to further increase this speed. Furthermore, individuals are using their genomes to learn about their (genetic) predispositions to diseases, their ancestries, and even their (genetic) compatibilities with potential partners. This trend has also caused the launch of health-related websites and online social networks (OSNs), in which individuals share their genomic data (e.g., OpenSNP or 23andMe). On the other hand, genomic data carries much sensitive information about its owner. By analyzing the DNA of an individual, it is now possible to learn about his disease predispositions (e.g., for Alzheimer's or Parkinson's), ancestries, and physical attributes. The threat to genomic privacy is magnified by the fact that a person's genome is correlated to his family members' genomes, thus leading to interdependent privacy risks.

This tutorial will help computer scientists better understand the privacy and security challenges in today's genomic era. We will first highlight the significance of genomic data and the threats for genomic privacy. Then, we will present the high level descriptions of the proposed solutions to protect the privacy of genomic data and we will discuss future research directions. We only require the attendees to have a slight background on cryptography and statistics.

Erman Ayday is an assistant professor of computer science at Bilkent University, Ankara, Turkey. Before that he was a post-doctoral Researcher at EPFL, Switzerland, in the Laboratory for Communications and Applications I (LCA1) led by Prof. Jean-Pierre Hubaux. Erman's research interests include privacy-enhancing technologies (including big data and genomic privacy), wireless network security, trust and reputation management, and applied cryptography.

Jean-Pierre Hubaux is a full professor at the School of Information and Communication Sciences of EPFL. Through his research, he contributes to laying the foundations and developing the tools to protect privacy in tomorrow's hyper-connected world. He is focusing notably on network privacy and security, with an emphasis on mobile/wireless networks and on data protection, with an emphasis on health-related data and especially genomic data.

Adversarial Data Mining: Big Data Meets Cyber Security

Abstract: Increasing amounts of cyber security incident data ranging from systems logs to vulnerability scan results are being collected. As more and more such data is collected, data mining techniques are becoming an essential tool for real-world cyber security solutions. One of the most important differences between applying data mining to cyber security and many other data mining applications is the existence of malicious adversaries that continuously adapt their behavior to make the data mining models ineffective. To address these concerns, over the last couple of years new and novel data mining techniques that are more resilient to such adversarial behavior are being developed in the data mining community. We believe that lessons learned as a part of this research direction would be beneficial for cyber security researchers who plan to apply data mining techniques in practice.

In this three-hour-long tutorial, we introduce the foundation, the techniques, and the applications of adversarial data mining to cyber security applications. We first introduce various data mining approaches proposed in the past to defend against active adversaries. We then discuss a game-theoretic framework to model the sequential actions of the adversary and the data miner while both parties try to maximize their utilities. Potential application of such techniques to intrusion detection and malware detection will be discussed in detail during the tutorial. Finally, we discuss how to use adversarial data mining ideas in practical cyber security applications and how to leverage existing big data management tools such as Spark for building data mining algorithms for cyber security.

Murat Kantarcioglu is a Professor of Computer Science and Director of the UTD Data Security and Privacy Lab at The University of Texas at Dallas. He holds MS and PhD degrees in Computer Science from Purdue University. Dr. Kantarcioglu's recent research focuses on using adversarial data mining techniques for fraud detection, cyber security and homeland security.

Bowie Xi received her Ph.D in statistics from the Department of Statistics at the University of Michigan, Ann Arbor in 2004. She is an associate professor in the Department of Statistics at Purdue University. Her research focuses on multidisciplinary work involving big datasets with complex structure from very different application areas including cyber security and Internet traffic.
Panel Discussion
Impact of Academic Security Research: Frogs in Wells, Storms in Teacups, or Raw Diamonds?

Panel Chair: Ahmad-Reza Sadeghi, TU Darmstadt, CYSEC, Germany
Panelists: Ross Anderson, University of Cambridge, UK
Robert Broberg, Cisco Systems Inc, USA
Bart Preneel, KU Leuven, Belgium
Anand Rajan, Intel Labs, USA
Greg Shannon, White House Office of Science & Technology Policy, USA

Abstract: Rapidly rising dependence on computerized technologies comes at a price of new vulnerabilities and attacks and poses a number of new security and privacy challenges compared to the last decade. In particular, in the post-Snowden era we are confronted with a significantly different threat quality: nation state adversaries and mass surveillance, growing hacker industry, aggressive data mining by cloud and social network providers inventing new fancy names for artificial intelligence, etc.

This panel will discuss the real-world impact (or lack thereof) of academic security research in light of these challenges. Have academic information security researchers lost the big picture, having limited view of practice (frogs in wells)? Have the tenure-track and grant-raising syndromes led to a tendency to overhype results of marginal or no real-world significance (storms in teacups)? Or are there highly valuable contributions that are still waiting to be discovered and shaped for high impact real-world deployment (raw diamonds)?

Ahmad-Reza Sadeghi is a full Professor of Computer Science at the Technische Universität Darmstadt, Germany, where he heads the Scientific Excellence Team of the Cybersecurity center TU Darmstadt (CYSEC).

Ross Anderson is Professor of Security Engineering at Cambridge University. He is one of the founders of a vigorously-growing new academic discipline, the economics of information security.

Robert Broberg is a Distinguished Engineer at Cisco Systems and an Associate Visiting Scholar at the University of Pennsylvania. As a member of Cisco’s Advanced Security Research and Government group he focuses on applied research of new approaches to secure the Internet.

Bart Preneel is full professor at the KU Leuven, where he heads the COSIC research group which has 60 members. His main research interests are cryptography, information security and privacy, and he frequently consults on these topics.

Anand Rajan is Director of the Emerging Security Lab at Intel Labs. He leads a team of senior technologists whose mission is to research novel security features that raise the assurance of platforms across the compute continuum (Cloud to Wearables).

Greg Shannon is the Chief Scientist for the CERT(r) Division at Carnegie Mellon University’s Software Engineering Institute. Shannon currently is on part-time detail to the White House Office of Science & Technology Policy as the Assistant Director for Cybersecurity Strategy.
Program

**ACM CCS 2016**

**CCS 2016 Main Conference, Tuesday, October 25, 2016**

<table>
<thead>
<tr>
<th>Track 1</th>
<th>Track 2</th>
<th>Track 3</th>
<th>Track 4</th>
<th>Track 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lecture Hall A</td>
<td>Lecture Hall B</td>
<td>Lecture Hall C</td>
<td>Lecture Hall D</td>
<td>Lecture Hall E</td>
</tr>
</tbody>
</table>

**Registration & Early Bird Coffee**

**Opening - Lecture Hall C**

**Keynote**

**Cybersecurity, Nuclear Security, Alan Turing, and Illogical Logic**

Keynote by Martin Hellman, Stanford University, US

ACM A.M. Turing Award Winner 2015

Lecture Hall C

**10.00 - 11.30**

<table>
<thead>
<tr>
<th>Session 1A</th>
<th>Session 1B</th>
<th>Session 1C</th>
<th>Session 1D</th>
<th>Tutorial 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blockchain I</td>
<td>Differential Privacy</td>
<td>Android Security</td>
<td>Hardware Protection</td>
<td>Program Anomaly Detection: Methodology and Practices</td>
</tr>
<tr>
<td>Ian Goldberg (University of Waterloo)</td>
<td>Prateek Mittal (Princeton University)</td>
<td>Xiaofeng Wang (Indiana University)</td>
<td>Taesoon Kim (Georgia Tech)</td>
<td></td>
</tr>
</tbody>
</table>

**Session 1A**

On the Security and Performance of Proof of Work Blockchains

Arthur Gervais (ETH Zürich), Ghassan O. Karame (NEC Laboratories Europe), Karl Wist, Vasileios Glykantzis, Hubert Ritzdorf and Srdjan Capkun (ETH Zürich)

A Secure Sharding Protocol For Open Blockchains

Loi Luu, Viswesh Narayanan, Chuadong Zheng, Kunal Baweja, Seth Gilbert and Prateek Saxena (National University of Singapore)

The Honey Badger of BFT Protocols

Andrew Miller (University of Maryland), Yu Xia (Tsinghua University), Kyle Croman, Elaine Shi (Cornell University) and Dawn Song (University of California)

**Session 1B**

Differential Privacy as a Mutual Information Constraint

Paul Caff and Laming Yu (Princeton University)

Advanced Probabilistic Couplings for Differential Privacy

Gilles Barthe (IMDEA Software Institute), Noémie Fong (ENS & IMDEA Software Institute), Marco Gaboardi (University at Buffalo, SUNY), Benjamin Grégoire (Inria), Justin Hsu (University of Pennsylvania) and Pierre - Yves Strub (IMDEA Software Institute)

Differentially Private Bayesian Programming

Gilles Barthe (IMDEA Software Institute), Gian Pietro Firtana, Marco Gaboardi (University at Buffalo, SUNY), Emilio Jesús Gallego Arias (CRI Mines – ParisTech), Andy Gordon (Microsoft Research), Justin Hsu (University of Pennsylvania) and Pierre - Yves Strub (IMDEA Software Institute)

**Session 1C**

The Misuse of Android Unix Domain Sockets and Security Implications

Yuru Shao (University of Michigan), Jason Ott (University of California, Riverside), Yuhang Jack Jia (University of Michigan), Zhiguo (University of California, Riverside) and Z. Morley Mao (University of Michigan)

Call Me Back! Attacks on System Server and System Apps in Android through Synchronous Callback

Kai Wang, Yuhang Zoung (University of Chinese Academy of Sciences, Beijing) and Feng Liu (The Pennsylvania State University)

**Session 1D**

Draco: A System for Uniform and Fine-grained Access Control for Web Code on Android

Gailz Senay Tunçay, Soteris Demetriou and Carl A. Gunter (University of Illinois at Urbana - Champaign)

**Session 1E**

Strong Non-Interference and Type-Directed Higher-Order Masking

Gilles Barthe (IMDEA Software Institute), Sonia Belaid (Thales Communications & Security), François Dupressoir (IMDEA Software Institute), Pierre - Alain Fouque (Université Rennes 1), Benjamin Grégoire (Inria), Pierre - Yves Strub (IMDEA Software Institute) and Rebecca Zucchini (Inria)

MERS: Statistical Test Generation for Side-Channel Analysis based Trojan Detection

Yuanwen Huang, Swarup Bhunia and Prabhat Misra (University of Florida)

Private Circuits III: Hardware Trojan-Resilience via Testing Implication

Stefan Dziembowski (University of Warsaw), Sebastian Faust (University of Bochum) and François - Xavier Standaert (Universität catholique de Louvain)

**11.30 - 12.00**

**Coffee Break**
<table>
<thead>
<tr>
<th>Time</th>
<th>Track 1</th>
<th>Track 2</th>
<th>Track 3</th>
<th>Track 4</th>
<th>Track 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.00</td>
<td>Session 2A Blockchain II</td>
<td>Session 2B Differentially Private Systems I Shai Halevi (IBM Research)</td>
<td>Session 2C Access Control Gail-Jooh Ahn (Arizona State University)</td>
<td>Session 2D Security and Persistence William Robertson (Northeastern University)</td>
<td>Invited Industrial Talk</td>
</tr>
<tr>
<td>13.30</td>
<td>Transparency Overlays and Applications Melissa Chase (Microsoft Research Redmond) and Sarah Meiklejohn (University College London)</td>
<td>Heavy Hitter Estimation over Set - Valued Data with Local Differential Privacy Zhan Qin (Qatar Computing Research Institute), Yin Yang (Hamad Bin Khalifa University), Ling Yu, Issa Khalil (Qatar Computing Research Institute), Xiaokui Xiao (Nanyang Technological University) and Kui Ren (SUNY Buffalo)</td>
<td>Mix&amp;Slice: Efficient Access Revocation in the Cloud Enrico Bacis (Università degli Studi di Bergamo), Sabrina De Capitani di Vimercati, Sara Foresti (Università degli Studi di Milano), Stefano Paraboschi, Marco Rosa (Università degli Studi di Bergamo) and Pierangela Samarati (Università degli Studi di Milano)</td>
<td>ProvUSB: Block - level Provenance - Based Data Protection for USB Storage Devices Dave (Jing) Tian (University of Florida), Adam Bates (University of Illinois at Urbana - Champaign), Kevin R.B. Butler (University of Florida) and Raju Ranganwami (Florida International University)</td>
<td></td>
</tr>
<tr>
<td>14.30</td>
<td>Tutorial 2</td>
<td>Tutorial 2</td>
<td>Tutorial 2</td>
<td>Tutorial 2</td>
<td>Tutorial 2</td>
</tr>
<tr>
<td>16.00</td>
<td>Lunch Break</td>
<td>Tutorial 2</td>
<td>Tutorial 2</td>
<td>Tutorial 2</td>
<td>Tutorial 2</td>
</tr>
</tbody>
</table>
Improvements to Secure Computation with Penalties
Ranjit Kamaresan, Vinod Vaikuntanathan and Prashant Nalini Vasudevan (MIT)

Amortizing Secure Computation with Penalties
Ranjit Kamaresan (MIT) and Iddo Bentov (Cornell)

MPC - Friendly Symmetric Key Primitives
Lorenzo Grassi, Christian Rechberger (TU Graz), Dragos Rotaru, Peter Scholl, Nigel F. Smart (University of Bristol)

Message-Recovery Attacks on Feistel-Based Format Preserving Encryption
Mihir Bellare (UC San Diego), Viet Tung Hoang and Stefano Tessaro (UC Santa Barbara)

On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN
Karthikeyan Bhargavan and Gaëtan Leurent (INRIA)

A Systematic Analysis of the Juniper Dual EC Incident
Stephen Chechoway (University of Illinois at Chicago), Jacob Maskiewicz (UC San Diego), Christina Garman (Johns Hopkins University), Joshua Fried (University of Pennsylvania), Shalman Cohnen (University of Pennsylvania), Matthew Green (Johns Hopkins University), Nadia Heninger (University of Pennsylvania), Ralf - Philipp Weinmann (Comecast), Eric Rescorla and Hovav Shacham (UC San Diego)

Scalable Graph-based Bug Search for Firmware Images
Qian Feng, Rundong Zhou, Chengcheng Xu, Yao Cheng, Brian Testa and Heng Yin (Syracuse University)

SmartWalk: Enhancing Social Network Security via Adaptive Random Walks
Yushan Liu (Princeton University), Shouding Ji (Georgia Tech) and Prateek Mittal (Princeton University)

High Fidelity Data Reduction for Big Data Security Dependency Analyses
Zhang Xu (College of William and Mary), Zhenyu Wu, Zichun Li, Kangkook Lee, Jungwhan Rhee, Xusheng Xiao, Pengyuan Xu (NEC Laboratories America), Haining Wang (University of Delaware) and Guofei Jiang (NEC Laboratories America)

TypeSanitizer: Practical Type Confusion Detection
Ishan Haller (Vrije Universiteit Amsterdam), Yuexin Jeon, Hui Peng, Mathias Payer (Purdue University), Cristiano Giuffrida, Herbert Bos and Erik van der Kooiwe (Vrije Universiteit Amsterdam)

CREDAL: Towards Locating a Memory Corruption Vulnerability with Your Core
Jun Xu (Pennsylvania State University), Dongliang Ma (Nanjing University), Ping Chen, Xinya Xing and Peng Liu (Pennsylvania State University)

Twice the Bits, Twice the Trouble: Vulnerabilities Induced by Migrating to 64 - Bit Platforms
Christian Wressnigg, Fabian Yamaguchi, Alwin Maier and Konrad Rieck (TU Braunschweig)

Agenda:
18.15 Meeting point is in front of the Conference Venue entrance (or you join us directly at the City Hall)
18.30 Doors open at Vienna City Hall (ticket = badge)
19.00 Opening
20.30 Award Ceremony
21.00 Poster/Demo Session

How to get there:
The CCS 2016 Team will guide you from the Conference Venue to the Vienna City Hall – it’s in walking distance (8-10min). You can either join us at the meeting point in front of the Conference Venue OR come directly to the Vienna City Hall (a map will be provided at the InfoDesk). Please wear your badge, it is your ticket for the dinner; the Vienna City Hall will check all tickets!

The Office of the Mayor of Vienna is inviting us to a Mayor’s Dinner at the Vienna City Hall. The dinner will take place in one of Vienna’s most beautiful ballrooms: the Festival Hall of the Vienna City Hall.

The Poster / Demo Session will take place during this evening. Also, all CCS 2016 awards will be presented, including the SIGSAC Awards, the CCS 2016 Best Paper Awards and the CCS 2016 Test-of-Time Awards.

Mayor’s Dinner @ Vienna City Hall
Poster / Demo Session
Award Ceremony

Mayor’s Dinner @ Vienna City Hall
Tuesday, October 25, 2016 | 18.30 – 23.00

The Office of the Mayor of Vienna is inviting us to a Mayor’s Dinner at the Vienna City Hall. The dinner will take place in one of Vienna’s most beautiful ballrooms: the Festival Hall of the Vienna City Hall.

The Poster / Demo Session will take place during this evening. Also, all CCS 2016 awards will be presented, including the SIGSAC Awards, the CCS 2016 Best Paper Awards and the CCS 2016 Test-of-Time Awards.

Agenda:
18.15 Meeting point is in front of the Conference Venue entrance (or you join us directly at the City Hall)
18.30 Doors open at Vienna City Hall (ticket = badge)
19.00 Opening
20.30 Award Ceremony
21.00 Poster/Demo Session

How to get there:
The CCS 2016 Team will guide you from the Conference Venue to the Vienna City Hall – it’s in walking distance (8-10min). You can either join us at the meeting point in front of the Conference Venue OR come directly to the Vienna City Hall (a map will be provided at the InfoDesk). Please wear your badge, it is your ticket for the dinner; the Vienna City Hall will check all tickets!

The Office of the Mayor of Vienna is inviting us to a Mayor’s Dinner at the Vienna City Hall. The dinner will take place in one of Vienna’s most beautiful ballrooms: the Festival Hall of the Vienna City Hall.

The Poster / Demo Session will take place during this evening. Also, all CCS 2016 awards will be presented, including the SIGSAC Awards, the CCS 2016 Best Paper Awards and the CCS 2016 Test-of-Time Awards.

Agenda:
18.15 Meeting point is in front of the Conference Venue entrance (or you join us directly at the City Hall)
18.30 Doors open at Vienna City Hall (ticket = badge)
19.00 Opening
20.30 Award Ceremony
21.00 Poster/Demo Session

How to get there:
The CCS 2016 Team will guide you from the Conference Venue to the Vienna City Hall – it’s in walking distance (8-10min). You can either join us at the meeting point in front of the Conference Venue OR come directly to the Vienna City Hall (a map will be provided at the InfoDesk). Please wear your badge, it is your ticket for the dinner; the Vienna City Hall will check all tickets!

The Office of the Mayor of Vienna is inviting us to a Mayor’s Dinner at the Vienna City Hall. The dinner will take place in one of Vienna’s most beautiful ballrooms: the Festival Hall of the Vienna City Hall.

The Poster / Demo Session will take place during this evening. Also, all CCS 2016 awards will be presented, including the SIGSAC Awards, the CCS 2016 Best Paper Awards and the CCS 2016 Test-of-Time Awards.

Agenda:
18.15 Meeting point is in front of the Conference Venue entrance (or you join us directly at the City Hall)
18.30 Doors open at Vienna City Hall (ticket = badge)
19.00 Opening
20.30 Award Ceremony
21.00 Poster/Demo Session

How to get there:
The CCS 2016 Team will guide you from the Conference Venue to the Vienna City Hall – it’s in walking distance (8-10min). You can either join us at the meeting point in front of the Conference Venue OR come directly to the Vienna City Hall (a map will be provided at the InfoDesk). Please wear your badge, it is your ticket for the dinner; the Vienna City Hall will check all tickets!

The Office of the Mayor of Vienna is inviting us to a Mayor’s Dinner at the Vienna City Hall. The dinner will take place in one of Vienna’s most beautiful ballrooms: the Festival Hall of the Vienna City Hall.

The Poster / Demo Session will take place during this evening. Also, all CCS 2016 awards will be presented, including the SIGSAC Awards, the CCS 2016 Best Paper Awards and the CCS 2016 Test-of-Time Awards.

Agenda:
18.15 Meeting point is in front of the Conference Venue entrance (or you join us directly at the City Hall)
18.30 Doors open at Vienna City Hall (ticket = badge)
19.00 Opening
20.30 Award Ceremony
21.00 Poster/Demo Session

How to get there:
The CCS 2016 Team will guide you from the Conference Venue to the Vienna City Hall – it’s in walking distance (8-10min). You can either join us at the meeting point in front of the Conference Venue OR come directly to the Vienna City Hall (a map will be provided at the InfoDesk). Please wear your badge, it is your ticket for the dinner; the Vienna City Hall will check all tickets!

The Office of the Mayor of Vienna is inviting us to a Mayor’s Dinner at the Vienna City Hall. The dinner will take place in one of Vienna’s most beautiful ballrooms: the Festival Hall of the Vienna City Hall.

The Poster / Demo Session will take place during this evening. Also, all CCS 2016 awards will be presented, including the SIGSAC Awards, the CCS 2016 Best Paper Awards and the CCS 2016 Test-of-Time Awards.

Agenda:
18.15 Meeting point is in front of the Conference Venue entrance (or you join us directly at the City Hall)
18.30 Doors open at Vienna City Hall (ticket = badge)
19.00 Opening
20.30 Award Ceremony
21.00 Poster/Demo Session

How to get there:
The CCS 2016 Team will guide you from the Conference Venue to the Vienna City Hall – it’s in walking distance (8-10min). You can either join us at the meeting point in front of the Conference Venue OR come directly to the Vienna City Hall (a map will be provided at the InfoDesk). Please wear your badge, it is your ticket for the dinner; the Vienna City Hall will check all tickets!

The Office of the Mayor of Vienna is inviting us to a Mayor’s Dinner at the Vienna City Hall. The dinner will take place in one of Vienna’s most beautiful ballrooms: the Festival Hall of the Vienna City Hall.

The Poster / Demo Session will take place during this evening. Also, all CCS 2016 awards will be presented, including the SIGSAC Awards, the CCS 2016 Best Paper Awards and the CCS 2016 Test-of-Time Awards.

Agenda:
18.15 Meeting point is in front of the Conference Venue entrance (or you join us directly at the City Hall)
18.30 Doors open at Vienna City Hall (ticket = badge)
19.00 Opening
20.30 Award Ceremony
21.00 Poster/Demo Session

How to get there:
The CCS 2016 Team will guide you from the Conference Venue to the Vienna City Hall – it’s in walking distance (8-10min). You can either join us at the meeting point in front of the Conference Venue OR come directly to the Vienna City Hall (a map will be provided at the InfoDesk). Please wear your badge, it is your ticket for the dinner; the Vienna City Hall will check all tickets!

The Office of the Mayor of Vienna is inviting us to a Mayor’s Dinner at the Vienna City Hall. The dinner will take place in one of Vienna’s most beautiful ballrooms: the Festival Hall of the Vienna City Hall.

The Poster / Demo Session will take place during this evening. Also, all CCS 2016 awards will be presented, including the SIGSAC Awards, the CCS 2016 Best Paper Awards and the CCS 2016 Test-of-Time Awards.

Agenda:
18.15 Meeting point is in front of the Conference Venue entrance (or you join us directly at the City Hall)
18.30 Doors open at Vienna City Hall (ticket = badge)
19.00 Opening
20.30 Award Ceremony
21.00 Poster/Demo Session

How to get there:
The CCS 2016 Team will guide you from the Conference Venue to the Vienna City Hall – it’s in walking distance (8-10min). You can either join us at the meeting point in front of the Conference Venue OR come directly to the Vienna City Hall (a map will be provided at the InfoDesk). Please wear your badge, it is your ticket for the dinner; the Vienna City Hall will check all tickets!
# ACM CCS 2016

## CCS 2016 Main Conference, Wednesday, October 26, 2016

<table>
<thead>
<tr>
<th>Time</th>
<th>Track 1</th>
<th>Track 2</th>
<th>Track 3</th>
<th>Track 4</th>
<th>Track 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:50</td>
<td>Lecture Hall A</td>
<td>Lecture Hall B</td>
<td>Lecture Hall C</td>
<td>Lecture Hall D</td>
<td>Lecture Hall E</td>
</tr>
</tbody>
</table>

### Registration & Early Bird Coffee

**Keynote**

Is it practical to build a truly distributed payment system?

Keynote by Ross Anderson, University of Cambridge, UK

Lecture Hall C

---

<table>
<thead>
<tr>
<th>Time</th>
<th>Session 5A</th>
<th>Session 5B</th>
<th>Session 5C</th>
<th>Session 5D</th>
<th>Tutorial 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:00</td>
<td>Secure MPC II</td>
<td>Physically Based Authentication</td>
<td>Web Security</td>
<td>Security Bug Finding</td>
<td></td>
</tr>
<tr>
<td>11:30</td>
<td>Claudio Orlandi (Aarhus University)</td>
<td>Erman Ayday (Bilkent University)</td>
<td>Ben Livshits (Microsoft Research)</td>
<td>Adam Doupe (Arizona State University)</td>
<td></td>
</tr>
</tbody>
</table>

### Session 5A: Secure MPC II

**Alternative Implementations of Secure Real Numbers**

Vassil Dimitrov (University of Calgary), Liisi Kerik (Cybernetica), Toomas Krips (STACC), Jaak Randmets and Jan Willenison (Cybernetica)

**Garbling Gadgets for Boolean and Arithmetic Circuits**

Marshall Ball, Tal Malkin (Columbia University) and Mike Rosulek (Oregon State University)

**Optimizing Semi - Honest Secure Multiparty Computation for the Internet**

Aner Ben - Efraim (Ben - Gurion University), Yehuda Lindell (Bar - Ilan University) and Eran Omri (Ariel University)

---

**MEMS Gyroscopes as Physical Unclonable Functions**

Oliver Willers, Christopher Huelt (Robert Bosch GmbH), Jorge Guiairos (Robert Bosch LLC – RTC) and Helmut Seidel (Siaurland University)

**On the Security and Usability of Segment-based Visual Cryptographic Authentication Protocols**

Tianhao Wang, Huangyi Ge, Omar Chowdhury, Hemanta K. Maji and Ninghui Li (Purdue University)

**Instant and Robust Authentication and Key Agreement among Mobile Devices**

Wei Xi (Xi'an Jiaotong University), Chen Qian (University of Kentucky), Jinsong Han, Kun Zhao (Xi'an Jiaotong University), Sheng Zhong (Nanjing University), Xiang - Yang Li (University of Science and Technology of China) and Jizhong Zhao (Xi'an Jiaotong University)

**Measurement and Analysis of Private Key Sharing in the HTTPS Ecosystem**

Frank Cangialosi (University of Maryland), Tiejiaojung Chung, David Cheffins (Northeastern University), Dave Levin (University of Maryland), Bruce M. Maggs (Duke University), Alan Mislove and Christo Wilson (Northeastern University)

**Chainsaw: Chained Automated Workflow-based Exploit Generation**

Abeer Alhusaini, Birhanu Estette, Rigel Gjomemo and V.N. Venkatakrishnan (University of Illinois at Chicago)

**CSPAutoGen: Black-box Enforcement of Content Security Policy upon Real-world Websites**

Xiang Pan (Northwestern University), Yinfen Liu, Xiang Pan, Yan Chen, Yang Hu (Northwestern University) and Tingting Zhou (Lehigh University)

**How I Learned to be Secure: a Census of Sources and Behavior**

Elisa M. Redmiles (University of Maryland), Sean Kross (Johns Hopkins University) and Michelle L. Mazurek (University of Maryland)

**Practical Detection of Entropy Loss in Pseudo - Random Number Generators**

Felix Döre and Vladimir Klebanov (Karlsruher Institute of Technology)

**Build It, Break It, Fix It: Contesting Secure Development**

Andrew Rouse, Michael Hicks, James Parker, Dave Levin, Michelle L. Mazurek (University of Maryland) and Piotr Mardziel (Carnegie Mellon University)

---

### Coffee Break

11:30

12:00

---

**THE ACM CCS 2016 PHOTO BOOTH**

Wanna take a special CCS Vienna souvenir with you?

Then visit our photo booth on the first floor! (next to the InfoDesk)

We invite you to create your personal CCS picture.
### Program

#### CCS 2016 Main Conference, Wednesday, October 26, 2016

<table>
<thead>
<tr>
<th>Track 1</th>
<th>Track 2</th>
<th>Track 3</th>
<th>Track 4</th>
<th>Track 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lecture Hall A</td>
<td>Lecture Hall B</td>
<td>Lecture Hall C</td>
<td>Lecture Hall D</td>
<td>Lecture Hall E</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Session 6A</th>
<th>Session 6B</th>
<th>Session 6C</th>
<th>Session 6D</th>
<th>Session 6E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone security using formal methods</td>
<td>Attestation</td>
<td>Mine your Literature</td>
<td>Security Studies</td>
<td>Tutorials &amp; Talks</td>
</tr>
<tr>
<td>Zhou Li (RSA Labs)</td>
<td>Kevin Butler (University of Florida)</td>
<td>Davide Balzarotti (Eurecom)</td>
<td>Chris Kanich (University of Illinois at Chicago)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lecture Hall B</th>
<th>Lecture Hall C</th>
<th>Lecture Hall D</th>
<th>Lecture Hall E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone security using formal methods</td>
<td>Attestation</td>
<td>Mine your Literature</td>
<td>Security Studies</td>
</tr>
<tr>
<td>Zhou Li (RSA Labs)</td>
<td>Kevin Butler (University of Florida)</td>
<td>Davide Balzarotti (Eurecom)</td>
<td>Chris Kanich (University of Illinois at Chicago)</td>
</tr>
</tbody>
</table>

---

**SandScout: Automatic Detection of Flaws in iOS Sandbox Profiles**
- Luke Dashefsky (North Carolina State University), Razvan Diaconescu, Mihai Chirita, University POLITEHNICA of Bucharest, Lucus Davi (TU Darmstadt), William Enck (North Carolina State University), and Ahmad - Reza Sadeghi (TU Darmstadt)

**Computational Soundness for Dalvik Bytecode**
- Michael Backes, Robert Kuenememnt (CISPA, Saarland University) and Esfandiar Mohammadi (ETH Zurich)

**SANA: Secure and Scalable Aggregate Network Attestation**
- Moreno Abravio, Mauro Conti (University of Padua), Ahmad Ibrahim (TU Darmstadt), Gregory Neven (IBM Research), Ahmad - Reza Sadeghi (TU Darmstadt) and Matthias Schunter (Intel Labs – Darmstadt)

**C-FLAT: Control - Flow Attestation for Embedded Systems Software**
- Tistig Abera (TU Darmstadt), N. Asookan (Aalto University), Lucas Davi (TU Darmstadt), Jan - Erik Ekborg (Trustonic), Thomas Nyman, Andrew Peverd (Aalto University), Ahmad - Reza Sadeghi (TU Darmstadt) and Gene Tsudik (University of California, Irvine)

---

**Session 7A**

**Secure MPC III**
- Stefan Katzenbeisser (TU Darmstadt)

**Session 7B**

**Side - Channel Attacks**
- Ahmad-Reza Sadeghi (TU Darmstadt)

**Session 7C**

**Acoustic Attacks**
- Amir Houmansadr (UMass Amherst)

**Session 7D**

**Protection Across Executions**
- Thorsten Holz (Ruhr-Universität Bochum)

---

**Lunch Break**

---

**Session 7E**

**High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority**
- Toshintori Araki, Jun Furukawa (NEC), Yehuda Lindell, Ariel Nof (Bar - Ilan University) and Kazuuma Ohara (NEC)

**Efficient Batched Oblivious PRF with Applications to Private Set Intersection**
- Vladimir Kolesnikov (Bell Labs), Ranjit Kamesaran (MIT), Mike Rosulek and Ni Trieu (Oregon State University)

**MASCOT: Faster Malicious Arithmetic Secure Computation with Oblivious Transfer**
- Marcel Keller, Emanuela Oriotti and Peter Scholl (University of Bristol)

---

**Session 8A**

**Covert Channels through Random Number Generator: Mechanisms, Capacity Estimation and Mitigations**
- Dmitry Evtushkin and Dmitry Ponomarev (SUNY Binghamton)

**Return-Oriented Flush - Reload Side Channels on ARM and Their Implications for Android Devices**
- Xiaokuan Zhang, Yuan Xiao and Yinqian Zhang (The Ohio State University)

**A Software Approach to Defeating Side Channels in Last - Level Caches**
- Ziiaq Zhou, Michael K. Reiter (University of North Carolina at Chapel Hill) and Yinqian Zhang (Ohio State University)

**Leave Your Phone at the Door: Side Channels that Can Read Factory Floor Secrets**
- Avesta Hojatj, Anka Adhikari, Katarina Struckmann, Edward Chou (University of Illinois at Urbana-Champaign), Thi Ngoc Tho Nguyen (Advanced Digital Sciences Center), Kushagra Madan, Marianne S. Wrstell, Carl A. Gunter and William P. King (University of Illinois at Urbana-Champaign)

**My Smartphone Knows What You Print: Exploring Smartphone - based Side - channel Attacks Against 3D Printers**
- Chen Song, Feng Lin, Zhongjie Ba, Kai Ren, Chi Zhou, Wenyao Xu (University at Buffalo, State University of New York)

---

**Session 8B**

**The Sounds of the Phones: Dangers of Zero - Effort Second Factor Login based on Ambient Audio**
- Balbo Strollo, Mallesh Shivraman, Prakash Shrestha and Nitesh Saxena (University of Alabama at Birmingham)

---

**Session 8C**

**Secure Code and Systems**
- Kevin Butler (University of Florida)

**FeatureSmith: Automatically Engineering Features for Malware Detection by Mining the Security Literature**
- Ziyun Zhu and Tudor Dumitras (University of Maryland)

**UniSan: Proactive Kernel Memory Initialization to Eliminate Data Leaksages**
- Kangjie Lu, Chengyu Song, Taeo Kim and Wenke Lee (Georgia Institute of Technology)

**iLock: Immediate and Automatic Locking of Mobile Devices against Data Theft**
- Tao Li, Yimin Chen, Jinhao Sun, Xiaoxing Jin, Yanhao Zhang (Arizona State University)

**Hypnoguard: Protecting Secrets across Sleep - Wake Cycles**
- Liangyong Zhao, Mohammad Maersmann (Concordia University)

---

**Session 8D**

**Currencies Special @ CCS 2016 (Part II)**
- On the Security and Scalability of Bitcoin's Blockchain
  - Ghasan O. Kanme (NEC Laboratories Europe, Germany)

---

**Tutorial 5**

**On the Security and Scalability of Bitcoin's Blockchain**
- Ghasan O. Kanme (NEC Laboratories Europe, Germany)

---

**Tutorial 4**

**An In-Depth Study of More Than Ten Years of Java Exploitation**
- Philipp Helzingre, Stefan Triller (Fraunhofer SIT), Alexandre Bartel (TU Darmstadt) and Eric Bodden (Paderborn University)

**The "Web/Local" Boundary Is Fuzzy: A Security Study of Chrome's Process-based Sandboxing**
- Yaoqi Jia, Zheng Long Chua, Hong Huang (National University of Singapore), Shuo Chen (Microsoft Research), Prateek Saxena and Zhenkai Liang (National University of Singapore)
<table>
<thead>
<tr>
<th>Time</th>
<th>Session/Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.00 – 16.30</td>
<td>Session 8A: Lattices and Obfuscation (Lecture Hall A)</td>
</tr>
<tr>
<td>16.30 – 18.00</td>
<td>Session 8B: Attacks and Defences (Lecture Hall B)</td>
</tr>
<tr>
<td>18.00 – 20.00</td>
<td>Session 8C: Phone Security (Lecture Hall C)</td>
</tr>
<tr>
<td>20.00 – 21.30</td>
<td>Session 8D: Infrastructure Attacks (Lecture Hall D)</td>
</tr>
</tbody>
</table>

**Track 1: Cryptographic Mechanisms**
- **Session 8A: Lattices and Obfuscation**
  - Stefan Dziembowski (University of Warsaw)
- **Session 8B: Attacks and Defences**
  - Yingqian Zhang (The Ohio State University)
- **Session 8C: Phone Security**
  - Manuel Egele (Boston University)
- **Session 8D: Infrastructure Attacks**
  - Zhiyun Qian (UC Riverside)

**Coffee Break**

**Track 2: Differential Privacy / Cryptography / Attacks**

**Track 3: Web/Mobile Security**

**Track 4: Secure Code and Systems**

**Track 5: Tutorials & Talks**

**Invited Industrial Talks**

**Panel Discussion**

Impact of Academic Security Research: Frogs in Wells, Storms in Teacups, or Raw Diamonds?
- Chair: Ahmad - Reza Sadeghi, TU Darmstadt, CYSSEC, Germany
- **Panelists:**
  - Ross Anderson, University of Cambridge, UK
  - Robert Broberg, Cisco Systems Inc
  - Bart Preneel, KU Leuven, Belgium, USA
  - Anand Rajan, Intel Labs, USA
  - Greg Shannon, White House Office of Science & Technology Policy, USA
- **Lecture Hall C**

**Traditional Viennese Dinner @ Heuriger**

"Man bringe den Spritzwein!" aka “Get me the sparkling wine!”

(Quote: Michael Häupl, Mayor of the City of Vienna)

The Dinner will take place at a “Heuriger” (traditional wine tavern), located on the outskirts of Vienna. Besides homegrown white wine and grape juices you will enjoy traditional Austrian food and music.

- **Meeting point:** Conference Venue entrance
- **Departure of the busses:** (20min drive) 22.00 – 24.00

Design requirements on resilient command control and signaling systems in the railway sector – first preliminary results of the CYSIS working group on IT security

Thorsten Borrmann (DB Netz AG, Germany) (16.30 – 17.15)

Experiences in Securing Smart Grids and their Operations

Klaus Kursawe (GridSec.org, The Netherlands) (17.15 – 18.00)
### Session 9A - Order-Revealing and Searchable Encryption (09.00 – 11.00)

**POPE: Partial Order Preserving Encoding**
Daniel S. Roche (United States Naval Academy), Daniel Apon (University of Maryland), Seung Geol Choi (United States Naval Academy) and Arkady Yerukhimovich (MIT Lincoln Laboratory)

**Σφως – Forward Secure Searchable Encryption**
Raphael Bost (Direction Générale de l’Armement – Maitrise de l’Information & Université de Rennes 1)

**What Else is Revealed by Order-Revealing Encryption?**
F. Betül Durak (Rutgers University), Thomas M. DuBuisson (Galos) and David Cash (Rutgers University)

### Session 9B - Authentication (09.30 – 11.00)

**Practical Anonymous Password Authentication and TLS with Anonymous Client Authentication**
Zhenfeng Zhang, Kang Yang (Chinese Academy of Sciences), Xueyan Hu (State Key Laboratory of Mathematical Engineering and Advanced Computing) and Yuchen Wang (Chinese Academy of Sciences)

**Efficient Cryptographic Password Hardening Services From Partially Oblivious Commitments**
Jonas Schneider, Nils Fleischhacker (CISPA, Saarland University), Dominique Schröder (Friedrich-Alexander-University Erlangen-Nürnberg) and Michael Bachs (Saarland University)

**A Comprehensive Formal Security Analysis of OAUTH 2.0**
Daniel Fett, Ralf Küsters and Guido Schmitz (University of Trier)

### Session 9C - Passwords (09.30 – 11.00)

**An Empirical Study of Mnemonic Sentence-based Password Generation Strategies**
Weining Yang, Ninghui Li, Omar Chowdhury, Aping Xiong and Robert W. Proctor (Purdue University)

**On the Security of Cracking-Resistant Password Vaults**
Maximilian Golla, Benedict Beucher and Markus Darmuth (Ruhr-University Bochum)

**Targeted Online Password Guessing: An Underestimated Threat**
Deng Wang, Zijian Zhang, Ping Wang (Peking University), Jeff Yan (Lancaster University) and Xinyi Huang (Pujian Normal University)

**Protecting Insecure Communications with Topology-aware Network Tunnels**
Georgios Kontaxis and Angelos D. Keromytis (Columbia University)

### Session 9D - Passwords (09.30 – 11.00)

**POPE: Partial Order Preserving Encoding**
Daniel S. Roche (United States Naval Academy), Daniel Apon (University of Maryland), Seung Geol Choi (United States Naval Academy) and Arkady Yerukhimovich (MIT Lincoln Laboratory)

**Σφως – Forward Secure Searchable Encryption**
Raphael Bost (Direction Générale de l’Armement – Maitrise de l’Information & Université de Rennes 1)

**What Else is Revealed by Order-Revealing Encryption?**
F. Betül Durak (Rutgers University), Thomas M. DuBuisson (Galos) and David Cash (Rutgers University)

### Coffee Break
<table>
<thead>
<tr>
<th>Time</th>
<th>Track 1</th>
<th>Track 2</th>
<th>Track 3</th>
<th>Track 4</th>
<th>Track 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.00</td>
<td>Specialized Crypto Tools</td>
<td>Specialized Crypto Tools</td>
<td>Measuring Security in the Wild</td>
<td>Network Security I</td>
<td>Tutorial E</td>
</tr>
<tr>
<td>11.00</td>
<td>Abhi Shelat (Northeastern University)</td>
<td>Abhi Shelat (Northeastern University)</td>
<td>Alejandro Russo (Chaimers Univ. of Technology)</td>
<td>Mohammad Mannan (Concordia University)</td>
<td>Tutorial 6</td>
</tr>
<tr>
<td>11.30</td>
<td>Editte Boyle (IDC Herzliya), Niv Gilboa (Ben Gurion University) and Yuval Ishai (Technion)</td>
<td>Editte Boyle (IDC Herzliya), Niv Gilboa (Ben Gurion University) and Yuval Ishai (Technion)</td>
<td>Stefano Calzavara, Alisse Rabitti and Michele Bugliesi (Università Ca’ Foscari Venezia)</td>
<td>Xiao Han, Nizar Kleir (Orange Labs) and Davide Balzarotti (Eurecom)</td>
<td>Erman Ayday (Bilkent University, Turkey) and Jean-Pierre Hubaux (EIFFL, Switzerland)</td>
</tr>
<tr>
<td>11.30</td>
<td>Dario Fiore (IMDEA Software Institute), Cedric Fournet (Microsoft Research), Esha Ghosh (Brown University), Marllof Kothweiss, Olga Ohrimenko and Bryan Parno (Microsoft Research)</td>
<td>Dario Fiore (IMDEA Software Institute), Cedric Fournet (Microsoft Research), Esha Ghosh (Brown University), Marllof Kothweiss, Olga Ohrimenko and Bryan Parno (Microsoft Research)</td>
<td>Lukas Weichselbaumer, Michele Spagnuolo, Sebastian Lekis and Arthur Jain (Google)</td>
<td>Duqing Liu (University of Delaware), Shuai Hao College of (William and Mary) and Haining Wong (University of Delaware)</td>
<td></td>
</tr>
<tr>
<td>11.30</td>
<td>Practical Non-Malleable Codes from l-more Extractable Hash Functions</td>
<td>Practical Non-Malleable Codes from l-more Extractable Hash Functions</td>
<td>Online tracking: A 1-million-site measurement and analysis</td>
<td>Identifying the Scan and Attack Infrastructure Behind Amplification DoS Attacks</td>
<td></td>
</tr>
<tr>
<td>11.30</td>
<td>Aggelos Kazias (University of Edinburgh), Feng-Hao Liu (Florida Atlantic University) and Yiannis Tsiolkous (University of Athens)</td>
<td>Aggelos Kazias (University of Edinburgh), Feng-Hao Liu (Florida Atlantic University) and Yiannis Tsiolkous (University of Athens)</td>
<td>Steven Englehardt and Arvind Narayanan (Princeton University)</td>
<td>Johannes Krupp, Michael Backes and Chistian Rosow (CISPA, Saarland University)</td>
<td></td>
</tr>
<tr>
<td>11.30</td>
<td>A Surfeit of SSH Cipher Suites</td>
<td>A Surfeit of SSH Cipher Suites</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.30</td>
<td>Maritn R. Albrecht, Juan Paul Doghriele, Torben Brandt Hansen and Kenneth G. Paterson (Royal Holloway, University of London)</td>
<td>Maritn R. Albrecht, Juan Paul Doghriele, Torben Brandt Hansen and Kenneth G. Paterson (Royal Holloway, University of London)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.30</td>
<td>Juraj Somorovsky (Ruhr University Bochum)</td>
<td>Juraj Somorovsky (Ruhr University Bochum)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.30</td>
<td>Attacking OpenSSL Implementation of ECDSA with a Few Signatures</td>
<td>Attacking OpenSSL Implementation of ECDSA with a Few Signatures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.30</td>
<td>Shuqin Fan (State Key Laboratory of Cryptology), Wenbo Wang and Qingsen Cheng (Luoyang University of Foreign Languages)</td>
<td>Shuqin Fan (State Key Laboratory of Cryptology), Wenbo Wang and Qingsen Cheng (Luoyang University of Foreign Languages)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.30</td>
<td>Lunch Break</td>
<td>Lunch Break</td>
<td>Lunch Break</td>
<td>Lunch Break</td>
<td>Lunch Break</td>
</tr>
<tr>
<td>13.00</td>
<td>A Unilateral-to-Mutual Authentication Compiler for Key Exchange (with Applications to Client Authentication in TLS 1.3)</td>
<td>A Unilateral-to-Mutual Authentication Compiler for Key Exchange (with Applications to Client Authentication in TLS 1.3)</td>
<td>Host of Troubles: Multiple Host Ambiguities in HTTP Implementations</td>
<td>Safely Measuring Tor</td>
<td>Adversarial Data Mining: Big Data Meets Cyber Security - Part I</td>
</tr>
<tr>
<td>13.00</td>
<td>Hugo Krawczyk (IBM Research)</td>
<td>Hugo Krawczyk (IBM Research)</td>
<td>Jianjun Chen (Tsinghua University), Jian Jiang (University of California, Berkeley), Haixin Duan (Tsinghua University), Nicholas Weaver (International Computer Science Institute), Tao Wan (Huawei Canada) and Vern Paxson (International Computer Science Institute)</td>
<td>Rob Jansen and Aaron Johnson (U.S. Naval Research Laboratory)</td>
<td>Murat Kantarcioglu (University of Texas at Dallas, USA) &amp; Bowet Xi (Purdue University, USA)</td>
</tr>
<tr>
<td>13.00</td>
<td>Attribute-based Key Exchange with General Policies</td>
<td>Attribute-based Key Exchange with General Policies</td>
<td>Accessorize to a Crime: Real and Stealthy Attacks on State-Of-The-Art Face Recognition</td>
<td>PREDATOR: Proactive Recognition and Elimination of Domain Abuse at Time-Of-Registration</td>
<td></td>
</tr>
<tr>
<td>13.00</td>
<td>Vladimir Kolosnikov (Bell Labs), Hugo Krawczyk (IBM Research), Yehuda Lindell (Bar-Ilan University), Alex Malzowof (Galits) and Tal Rabin (IBM Research)</td>
<td>Vladimir Kolosnikov (Bell Labs), Hugo Krawczyk (IBM Research), Yehuda Lindell (Bar-Ilan University), Alex Malzowof (Galits) and Tal Rabin (IBM Research)</td>
<td>Mahmoud Sharif, Su-Ming Ho, Naveen Raveendran and Tony Cheung (University of California, Berkeley)</td>
<td>Shuang Hao (UC Santa Barbara), Alex Kandchelian (UC Berkeley), Brad Miller (Google), Vern Paxson (UC Berkeley) and Nick Feamster (Princeton University)</td>
<td></td>
</tr>
<tr>
<td>13.00</td>
<td>Identity-Concealed Authenticated Encryption and Key Exchange</td>
<td>Identity-Concealed Authenticated Encryption and Key Exchange</td>
<td>Accessorize to a Crime: Real and Stealthy Attacks on State-Of-The-Art Face Recognition</td>
<td>Stemming Downlink Leakage from Training Sequences in Multi-User MIMO Networks</td>
<td></td>
</tr>
<tr>
<td>13.00</td>
<td>Yunlei Zhao (Fudan University)</td>
<td>Yunlei Zhao (Fudan University)</td>
<td>Mahmoud Sharif, Su-Ming Ho, Naveen Raveendran and Tony Cheung (University of California, Berkeley)</td>
<td>Yanlong Mao, Yuan Zhang and Sheng Zhong (Nanjing University)</td>
<td></td>
</tr>
<tr>
<td>13.00</td>
<td>Generic Attacks on Secure Outsourced Databases</td>
<td>Generic Attacks on Secure Outsourced Databases</td>
<td>Breaking Web Applications Built On Top of Encrypted Data</td>
<td>Xiaojing Liao (Georgia Institute of Technology), Sumayah Alhwa, Kan Yuan, Luyi Xing, XiaoFeng Wang (Indiana University Bloomington), Shuang Hao (University of California Santa Barbara) and Ruheem Beyah (Georgia Institute of Technology)</td>
<td></td>
</tr>
<tr>
<td>13.00</td>
<td>Georgios Kellaris (Harvard University), George Kellos (Boston University), Kobbi Nissim (Ben Gurion University) and Adam O’Neill (Georgetown University)</td>
<td>Georgios Kellaris (Harvard University), George Kellos (Boston University), Kobbi Nissim (Ben Gurion University) and Adam O’Neill (Georgetown University)</td>
<td>Paul Grabb (Cornell University), Richard McPherson (University of Texas, Austin), Muhammed Naveed (University of Southern California), Thomas Ristenpart and Vitaly Shmatikov (Cornell Tech)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# ACM CCS 2016

## CCS 2016 Main Conference, Thursday, October 27, 2016

<table>
<thead>
<tr>
<th>Track 1</th>
<th>Track 2</th>
<th>Track 3</th>
<th>Track 4</th>
<th>Track 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lecture Hall A</td>
<td>Lecture Hall B</td>
<td>Lecture Hall C</td>
<td>Lecture Hall D</td>
<td>Lecture Hall E</td>
</tr>
</tbody>
</table>

### Session 12A: Secure Protocols
- **Lecture Hall A**
- **Session 12A**
  - Session 12A Secure Protocols
  - Matteo Maffei (Saarland University)
  - A Protocol for Privately Reporting Ad Impressions at Scale
    - Matthew Green (Johns Hopkins University), Watson Ladd (University of California Berkeley) and Jan Miers (Johns Hopkins University)
  - Secure Stable Matching at Scale
    - Jack Doerner, David Evans and Abhi Shelat (University of Virginia)
  - BelenosRF: A Non-Interactive Receipt-Free Electronic Voting Scheme
    - Pyros Chaidos, (University College London), Véronique Cortier (CNRS), Georg Fuchsbauer (Inria) and David Galindo (University of Birmingham)

### Session 12B: DSA/ECDSA
- **Session 12B**
  - DSA/ECDSA
  - Markulf Kohlweiss (Microsoft Research)
  - ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels
    - Daniel Genkin (Technion), Lev Puchmanov, Iasmar Pipman, Eran Tromer (Tel Aviv University) and Yuval Yarom (The University of Adelaide)
  - „Make Sure DSA Signing Exponentiations Really Are Constant-Time“
    - César Pereida García (Aalto University), Billy Bob Brumley (Tampere University of Technology) and Yuval Yarom (The University of Adelaide)
  - On the Provable Security of (EC)DSA Signatures
    - Manuel Fersch, Elke Kiltz and Bertram Poettering (Ruhr University Bochum)

### Session 12C: Even more Attacks
- **Session 12C**
  - Even more Attacks
  - Mathias Payer (Purdue University)
  - Android ION Hazard: the Curse of Customizable Memory Management System
    - Hang Zhang, Dongdong She and Zhiyan Qian (University of California, Riverside)
  - Coverage-based Greybox Fuzzing as Markov Chain
    - Marcel Boehme, Van-Thuan Pham and Abhik Roychoudhury (National University of Singapore)
  - SFADiff: Automated Evasion Attacks and Fingerprinting Using Blackbox Differential Automata Learning
    - George Argyros (Columbia University), Ioannis Stais (University of Athens), Siyuan Jana, Angelos Keromytis (Columbia University) and Aggelos Kiayias (University of Edinburgh)

### Session 12D: Censorship Resistance
- **Session 12D**
  - Censorship Resistance
  - Slithen: Perfectly imitated decoy routing through traffic replacement
    - Cecilia Bocovich and Ian Goldberg (University of Waterloo)
  - Practical Censorship Evasion Leveraging Content Delivery Networks
    - Hadi Zolfaghari and Amir Houmansadr (UMass Amherst)
  - GAME OF DECOYS: Optimal Decoy Routing Through Game Theory
    - Milad Navaei and Amir Houmansadr (UMass Amherst)

### Tutorials & Talks
- **Tutorial 7**
  - Adversarial Data Mining: Big Data Meets Cyber Security - Part II
    - Murat Kantarcioglu (University of Texas at Dallas, USA) & Bowei Xi (Purdue University, USA)

### CCS Business Meeting
- **Lecture Hall C**
  - CCS Business Meeting

### Sightseeing Tour
- **Lecture Hall C**
  - Sightseeing Tour
    - (For ticket holders only! Window for purchase closed on October 21, 2016!)
    - 19.05 Meeting point in front of the Conference Venue entrance
    - 19.15 Departure of the busses, start of the tour
    - 20.45 End of the tour at the Conference Venue
A Behavioural Authentication System for Mobile Users
Md Mohshud Islam and Reihaneh Safavi-Naini (University of Calgary)

A Keyless Efficient Algorithm for Data Protection by Means of Fragmentation
Katarzyna Kapusta, Gerard Memmi and Hassan Noua (Telecom ParisTech)

Accuracy vs. Time Cost: Detecting Android Malware through Pareto Ensemble Pruning
Lingling Fan (East China Normal University), Minhui Xue (East China Normal University and NYU Shanghai), Sen Chen, Libao Xu (East China Normal University), Haquin Zhu (Shanghai Jiao Tong University)

An Educational Network Protocol for Covert Channel Analysis Using Patterns
Steffen Wendel (Fraunhofer FKIE / Worms University of Applied Sciences) and Wojciech Mazurczyk (Warsaw University of Technology)

Attack on Non-Linear Physical Unclonable Function
Jing Ye, Tu Hu, and Xiaowei Li (State Key Laboratory of Computer Architecture, Institute of Computing Technology, Chinese Academy of Sciences)

ConcurORAM: High-Throughput Parallel Multi-Client ORAM
Anrin Chakraborti and Radu Sion (Stony Brook University)

DataLair: A Storage Block Device with Plausible Deniability
Anrin Chakraborti, Chen Chen and Radu Sion (Stony Brook University)

DroidShield: Protecting User Applications from Normal World Access
Darius Suciu and Radu Sion (Stony Brook University)

Efficient Cross-User Chunk-Level Client-Side Data Deduplication with Symmetrically Encrypted Two-Party Interactions
Chia-Mu Yu (National Chung Hsing University)

Fingerprinting Tor Hidden Services
Aya Mitsve, Andriy Panchenko (University of Luxembourg), Fabian Lamez (Huf, Huf & Fara GmbH & Co. KG), Martin Henze (RWTH Aachen University), Klaus Wehrle (RWTH Aachen University) and Thomas Engel (University of Luxembourg)

I Don’t Want That Content! On the Risks of Exploiting Bitcoin’s Blockchain as a Content Store
Roman Matzutt, Oliver Hofhild, Martin Henze, Robin Ravel, Jan Henrik Ziegeldorf and Klaus Wehrle (RWTH Aachen University)

Identifying Dynamic Data Structures in Malware
Thomas Rappprecht (University of Bamberg), Xi Chen (Vrije Universiteit Amsterdam), David H. White (University of Bamberg), Jan Tobias Mälich (KU Leuven), Herbert Bos (Vrije Universiteit Amsterdam) and Gerald Lütgen (University of Bamberg)

Improved Markov Strength Metrics for Passwords
Harshad Tegumadre, Vijayanand Banahatti and Sachin Lodha (TCS Research)

Insights of Antivirus Relationships when Detecting Android Malware: A Data Analytics Model
Igancio Martin, Jose Alberto Hernandez (Universidad Carlos III de Madrid), Sergio de Los Santos and Antonio Guzmán (Telefónica Digital Identity & Privacy)

KKRay: Introspecting the Kernel for Rootkit Timing Footprints
Chen Chen, Darius Suciu and Radu Sion (Stony Brook University)

Locally Virtualized Environment for Mitigating Ransomware Threat
Manoh Shukla, Susapa Mondal and Sachin Lodha (TCS Research)

Mapping the Landscape of Large-Scale Vulnerability Notifications
Ben Stock, Giancarlo Pellegrino, Christian Rossow (CISPA, Saarland University), Martin Johns (SAP SE) and Michael Backes (CISPA, Saarland University & MPI-SWS)

Phishing Website Detection with a Multiphase Framework to Find Visual Similarity
Omid Asaadi (University of Texas at Arlington) and Matthew Wright (Rochester Institute of Technology)

Privacy Enhanced Secure Location Verification
Md Mamunur Rashid Akhan and Rei Safavi-Naini (University of Calgary)

Re-Thinking Risks and Rewards for Trusted Third Parties
Jan-Ole Maichow, Benjamin Gaedken and Volker Roth (Freie Universität Berlin)

RIA: an Audition-based Method to Protect the Runtime Integrity of MapReduce Applications
Yangzhi Wang and Yulong Shen (Xi’an Jiaotong University)

Security Enhanced Administrative Role Based Access Control
Rajkumar P.V. (Texas Southern University) and Ravi Sundha (University of Texas at San Antonio)

(Semi-)Supervised Machine Learning Approaches for Network Security in High-Dimensional Network Data
Pedro Casas, Alessandro D’Alcozno, Giuseppe Settanni (AIT Austrian Institute of Technology), Pernondemico Fudino (Eurecat Technology Centre of Catalonia) and Florian Slopik (AIT Austrian Institute of Technology)

Static ROP Chain Detection Based on Hidden Markov Model Considering ROP Chain Integrity
Toshikuni Usui (NTT Secure Platform Laboratories), Tomonori Inase (NTT Security(Japan)KK), Makoto Iwamura, Takeshi Yada (NTT Secure Platform Laboratories)

The ART of App Compartmentalization
Michael Backes (CISPA, Saarland University & MPI-SWS), Sven Bugiel, Jie Huang and Oliver Schranz (CISPA, Saarland University)

Towards Automating the Generation of Malware Analysis Reports Using the Sandbox Logs
Bo Sun, Akinori Fujino and Tatsuya Mori (Waseda University)

Toward Collaboratively Supporting Decision Makers in Choosing Suitable Authentication Schemes
Peter Mayer, Stephan Neumann (Technische Universität Darmstadt) and Melanie Vollkorn (Technische Universität Darmstadt & Karlstad University)

Towards Exposing Internet of Things: A Roadmap
Vinay Sachdevand, Jinghui Toh, Shuchar Sithoni, Asaf Shaltiti (Ben-Gurion University of the Negev) and Yusaf Elvoci (Singapore University of Technology and Design)

Towards Highly Interactive Honeypots for Industrial Control Systems
Stephan Lau, Johannes Klick, Stephan Arndt and Volker Roth (Freie Universität Berlin)

Towards Privacy-Preserving Biometric Identification in Cloud Computing Environments
Changhee Hahn and Junbeom Hur (Department of Computer Science and Engineering, Korea University)

VUDEC – A Framework for Vulnerability Management in Decentralized Communication Networks
Michael Steinke (Universität der Bundeswehr), Stefan Metzger (Leibniz SupercomputingCentre) and Wolfgang Hommel (Universität der Bundeswehr)

Weighing in eHealth Security — A Security and Privacy Study of Smart Scales
Martin Knüter, David Aspinall and Maria Wolters (University of Edinburgh)

WIPING: Wi-Fi signal-based PIN Guessing attack
Seunghun Cha, Jaewoo Park, Geumhwon Cho (Sungkyunkwan University), Jun Ho Huh (Honeywell ACS Lab) and Hyungadick Kim (Sungkyunkwan University)

Easy Deployment of a Secure Internet Architecture for the 21st Century - How hard can it be to build a secure Internet?
Eran Ucan, Raphael M. Reischuk and Adrian Perrig (ETH Zurich)

High-Throughput Secure Three-Party Computation of Kerberos Ticket Generation
Toshinori Anaki (NEC Corporation), Assaf Banak (Bar-Ilan University), Jan Furskawka (NEC Corporation), Yehuda Lindell, Ariel Nof (Bar-Ilan University) and Kazuma Ohara (NEC Corporation)

Integrating MPC in Big Data Workflows
Nikolaj Volgashchev (Boston University), Malte Schwarzkopf (MIT CSAIL), Andrei Lapets, Mayank Varia and Azer Bestavros (Boston University)

OffPAD — Offline Personal Authenticating Device with Applications in Hospitals and e-Banking
Denis Migdal (ENSICAEN), Christian Johannes and Aadan Jauan (University of Oslo)

Starving Permission-Hungry Android Apps Using SecuRank
Vincent Taylor and Ivan Martinovic (University of Oxford)
6th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM 2016)  
PC Chairs: Long La (Stony Brook University, USA), Mohammad Munawar (Concordia University, USA)  
07.30 – 09.00 Registration & Early Bird Coffee  
09.00 – 10.30 Welcome and Session 1: Keynote  
Keynote: Hardware Isolation for Trusted Execution. Jan-Erik Ekborg (Trustonic)  
10.30 – 11.00 Coffee Break  
11.00 – 12.30 Session 2: Studies and Analyses  
Session Chair: Konstantin Beznosov (University of British Columbia)  
Secure Containers in Android: the Samsung KNOX Case Study. Uri Kanonov and Avishai Wool (Tel Aviv University)  
White Rabbit in Mobile: Effect of Unsecured Clock Source in Smartphones. Shingo Furuk, Aliaf Shaik (TU Berlin/Telekom Innovation Labs), Raveeshankar Borkaonkar (Oxford University) and Jean-Pierre Seifert (TU Berlin/Telekom Innovation Labs)  
What You See Isn’t Always What You Get: A Measurement Study of Usage Fraud on Android Apps. Wei Liu, Yueqin Zhang (Tsinghua University), Zhou Li (ACM Member) and Haxian Duan (Tsinghua University)  
CRIOS: Toward Large-Scale iOS Application Analysis. Demidova Orskog, Manuel Egele and Matthias Buchler (Boston University)  
12.30 – 14.00 Lunch  
14.00 – 15.30 Session 3: Privacy  
Session Chair: Manuel Egele (Boston University)  
SecuRank: Starving Permission-Hungry Apps Using Contextual Permission Analysis. Vincent Taylor and Ivan Martinovic (University of Oxford)  
Securing Recognizers for Rich Video Applications. Christopher Thompson and David Wagner (University of California, Berkeley)  
23rd ACM Conference on Computer and Communications Security  
Hofburg Imperial Palace, Vienna, Austria, October 24-28, 2016  
On a (Per)Mission: Building Privacy Into the App Marketplace. Hannah Quay-De La Valley, Paige Selby and Shreem Krishnamurthi (Brown University)  
Exploiting Phone Numbers and Cross-Application Features in Targeted Mobile Attacks. Srishti Gupta (Indraprastha Institute of Information Technology, Delhi), Payas Gupta (School of Information Systems, Singapore Management University), Mustaque Ahamad (Georgia Institute of Technology & New York University Abu Dhabi) and Fomunumangam Kamaragurub (IITD)  
15.30 – 16.00 Coffee Break  
16.00 – 17.40 Session 4: Attacks and Defenses  
Session Chair: William Enck (North Carolina State University)  
Hardened Setup of Personalized Security Indicators to Counter Phishing Attacks in Mobile Banking. Claudio Marforio, Ramya Masti (ETH Zurich), Claudio Soriente (Telefónica), Kostas Kostis and Sujan Capugan (ETH Zurich)  
Picasso: Lightweight Device Class Fingerprinting for Web Clients. Elie Burstein, Artem Malyshev, Tadek Pietraszek and Kari Thomas (Google)  
Detecting Misuse of Google Cloud Messaging in Android Badware. Mansour Almadi, Battista Baggio (University of Cagliari), Steven Arzt (Technische Universität Darmstadt), Davide Ariu and Giorgio Giacinto (University of Cagliari)  
On the CCA (in)security of MTProtocol (short paper) Jakob Jakobsen and Claudio Orlandi (Aarhus University)  
Breaking TETRA Location Privacy and Network Availability. (short paper) Martin Pleffer, Jan-Pascal Kwietek, Jiska Claassen, Robin Klohe and Matthias Hollick (Secure Mobile Networking Lab, TU Darmstadt)  
10.30 – 11.00 Coffee Break  
11.00 – 12.30 Session 2: Security and Network Privacy  
Session Chair: Ian Goldberg (University of Waterloo)  
Generating Secret Keys from Biometric Body Impedance Measurement. Marc Roeschlin, Ivo Stangosse, Ivan Martinovic (University of Oxford), Gene Tsudik (University of California) and Kasper Bonne Rasmussen (University of Oxford)  
That's the Way the Cookie Crumbles: Evaluating HTTPS Enforcing Mechanisms. Junho Suh, Swati Gedania, Carlos Manzalini (University of California), Jason Polakis (University of Illinois at Chicago)  
Detecting Communities under Differential Privacy. Hua-Hui Nguyen, Abdessamad Imine and Michael Kozic (LORIA/INRIA Nancy)  
Poisoning the Well - Exploring the Great Firewall’s Poisoned DNS Responses. Oliver Firsan (University of Oxford), Alex Duer (Oxford Internet Institute) and Jess Wright (University of Oxford)  
12.30 – 13.45 Lunch  
07.30 – 08.25 Registration & Early Bird Coffee  
08.25 – 10.30 Welcome & Session 1: User Privacy  
Session Chair: Yuzan Zhou (Peking University)  
An Efficient and Robust Social Network De-anonymization Attack. Gabhor Gyorgy Gulyas (INRIA), Benoît Simon and Sándor Imre (BME)  
Control Versus Effort in Privacy Warnings for Webforms. Kat Krol (University of London) and Según Preuhs (Microsoft Research)  
On Profile Linkability despite Anonymity in Social Media Systems. Michael Baches, Pascal Berrang (CISPA, Saarland University), Oana Goga (MPI-SWS), Cristina Gammata (MPI-SWS) and Praveen Manoharan (CISPA, Saarland University)  
Disguised Chromium Browser: Robust browser, Flash and Canvas Fingerprinting Protection. Martin Stopczynski, Peter Baumann, Stefan Katzenbeisser (TU Darmstadt) and Erik Terp (University of Birmingham)  
Predicting Mobile App Privacy Preferences with Psychographics. Andrew McNamara, Abuil Venma, Jon Stallings and Jessica Staddon (N.C. State Univ.)  
15.30 - 16.00 Coffee Break  
16.00 - 18.10 Session 4: Data privacy and Anonymous Communication  
Session Chair: Hans Poos (Kapirodamititmir (KTH, Sweden)  
(The Futility of) Data Privacy in Content-Centric Networking. Christopher A. Wood, Cesar Gaiti and Gene Tsudik (University of California Irvine)  
Elka: Scalable Privacy-Preserving Plagiarism Detection. Nik Unger, Sahiti Thandra and Ian Goldberg (University of Waterloo)  
ABRA CADABA: Magically Increasing Network Utilization in Tor by Avoiding Bottlenecks. John Goddard, Michael Schlep and Nicholas Hopper (University of Minnesota)  
TASP: Towards Anonymity Sets that Persist. Jamie Hayes (University of London), Carmela Troncoso (IMDEA Software Institute) and George Danezis (University College London)  
PRF: A Low-Latency and Tracking-Resistant Protocol for Local-Area Anonymous Communication. Ludovic Barman (EPFL), Mahdi Zamani (Lake Univ.), Isao Dacosta (EPFL, Switzerland), Joan Feigenbaum (Yale Univ.), Bryan Ford, Jean-Pierre Hubaux (EPFL) and David Wilksnay (Facebook)  
Privacy-Preserving Lawful Contact Chaining. Aaron Segal, Joan Feigenbaum (Yale Univ.) and Bryan Ford (EPFL)
<table>
<thead>
<tr>
<th>Time</th>
<th>Session/Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>07.30 – 09.00</td>
<td>Registration &amp; Early-Bird Coffee</td>
</tr>
<tr>
<td>09.00 – 10.30</td>
<td>Welcome and Session 1: Keynote speech</td>
</tr>
<tr>
<td>10.30 – 11.00</td>
<td>Keynote speech: Information Sharing and Cybersecurity Economics</td>
</tr>
<tr>
<td>11.00 – 12.30</td>
<td>Session 2: Models for Information Sharing</td>
</tr>
<tr>
<td>12.30 – 14.00</td>
<td>Lunch</td>
</tr>
<tr>
<td>14.00 – 15.00</td>
<td>Session 3: Tools for Information Sharing</td>
</tr>
<tr>
<td>15.30 – 16.00</td>
<td>Coffee Break</td>
</tr>
<tr>
<td>16.00 – 17.30</td>
<td>Session 4: Real-World Studies</td>
</tr>
<tr>
<td>14.20 – 14.50</td>
<td>Industry Talk</td>
</tr>
<tr>
<td>14.50 – 15.50</td>
<td>Session 3: Modeling and Evaluation of Moving Target Defenses (I)</td>
</tr>
<tr>
<td>15.50 – 16.05</td>
<td>Coffee Break</td>
</tr>
<tr>
<td>16.05 – 17.35</td>
<td>Session 4: Modeling and Evaluation of Moving Target Defenses (II)</td>
</tr>
<tr>
<td>17.35 – 17.40</td>
<td>Wrap up</td>
</tr>
</tbody>
</table>

**Session 1: New Moving Target Defenses (I)**

- **Privacy Risk in Cybersecurity Data Sharing.** Jaspreet Bhatia, Travis Breax (CMU), Liora Friedberg (UPenn), Hanan Hikishi and Daniel Smulian (CMU)
  - Data quality challenges and future research directions in threat intelligence sharing practice. Christian Sillaber, Clemens Sauerwein and Ruth Bress (University of Innsbruck)
  - Measuring the Impact of Sharing Abuse Data with Web Hosting Providers. Marie Vazek, Matthew Weeden and Tyler Moore (University of Tulsa)

- **A Model for Secure and Mutually Beneficial Software Vulnerability Sharing.** Alex Davidson, Gregory Finn and Carlos Cid (Royal Holloway University of London)

- **Collaborative Incident Handling Based on the Blackboard-Pattern.** Nadine Herold, Holger Kinkelte and Georg Carle (Technical University of Munich)

- **Private Sharing of IOCs and Sightings (short paper).** Tim K. van de Kamp, Andreas Peter, Maarten H. Everts and Willem Jenker (University of Twente)

- **Managing Data Sharing in OpenStack Swift with Over-Encryption.** Enrico Bats (Università degli Studi di Bergamo), Sabrina De Capitani di Vimercati, Sara Foresti (Università degli Studi di Milano), Daniele Gattadore, Stefano Paraboschi, Marco Rosa (Università degli Studi di Bergamo), Pierangela Samarati (Università degli Studi di Milano) and Alessandro Saudio (Università degli Studi di Bergamo)

- **MISP - The design and implementation of a collaborative threat intelligence sharing platform.** Cynthia Wagner (RESTENA Foundation), Alexandra Dulasnoy, Gerald Wagen and Andras Imboly (CIRCL)

- **Have No PHEAR: Networks without Identifiers.** Richard Skowyra, Kevin Bauer, Veer Dedhia and Hamed Oskhvat (MIT Lincoln Laboratory)

- **Towards Cost-Effective Moving Target Defense Against DDoS and Covert Channel Attacks.** Huangyan Wang, Fei Li and Songxing Chen (GMU)

- **A Moving Target Defense Approach to Disrupting Stealthy Botnets.** Sridhar Venkatase, Massimiliano Albanese (GMU), George Cybenko (Dartmouth College) and Sushil Jajodia (CEM)

- **Multi-dimensional Host Identity Anonymization for Defeating Skilled Attackers.** Jafar Haadi Jafarian, Amiressa Niakehtalaki, Ehab Al-Shaer and Qi Duan (UNCC)

- **SDN based scalable MTD solution in Cloud.** Ankur Chowdhary, Sandeep Fisuray and Dujing Huang (ASU)

- **A Moving Target Defense Framework for Distributed Systems:** Nos Ahmed (AFRL) and Bhanu Bhargava (Purdue University)

- **Mayflies: A Moving Target Defense Framework for Distributed Systems (short paper).** Nos Ahmed (AFRL) and Bhanu Bhargava (Purdue University)

- **Automated Effectiveness Evaluation of Moving Target Defenses: Metrics for Missions and Attacks.** Nos Ahmed (AFRL) and Bhanu Bhargava (Purdue University)

- **Towards Cost-Effective Moving Target Defense (II).** Chen Liu (Intel)
SafeConfig & TIS

Testing and Evaluation for Active & Resilient Cyber Systems (SafeConfig 2016)
Monday, October 24, Lecture Hall H
PC Chairs: David Manz (Pacific Northwest National Laboratory, USA), Anoop Singhal (National Institute of Standards and Technology, USA), Nick Mullari (Pacific Northwest National Laboratory, USA)

10.30 – 11.00 Coffee Break
11.00 – 12.30 Session 1
Session Chair: Nick Mullari (Pacific Northwest National Laboratory)

AHEAD: A New Architecture for Active Defense. Fabio De Gaspari (Sapienza Univ), Sushil Jajodia (George Mason Univ), Luigi V. Mancini and Agostino Panico (Sapienza Univ)

A One-Year Perspective on Exposed In-memory Key-Value Stores. Tobias Pfeig, Anja Feldmann and Matthias Pitschke (TU Berlin)

Towards Automated Verification of Active Cyber Defense Strategies on Software Defined Network. Mohammed Alsaleh and Ehab Al-Shaar (UNCC)

12.30 – 14.00 Lunch Break

14.00 – 15.30 Session 2
Session Chair: David Manz (Pacific Northwest National Laboratory)

Firewalling Scenic Routes: Preventing Data Exfiltration via Political and Geographic Routing Policies. Kevin Benton and L. Jean Camp (Indiana Univ)

An Iterative and Toolchain-Based Approach to Automate Scanning and Mapping Computer Networks. Stefan Marksteiner, Harald Lernbeiss and Bernhard Jandl-Scherf (Joanneum Research)

A Graph-Based Impact Metric for Mitigating Lateral Movement Cyber Attacks. Emilie Parvinte, John R. Johnson and Chaomel Lo (PNNL)

15.30 – 16.00 Coffee Break

16.00 – 17.30 Panel Discussion: Testing and Evaluation for Active and Resilient Cyber Systems
Session Chair: David Manz (Pacific Northwest National Laboratory)

Panelists:
• Bob Cowles (Principal, BrightLite Information Security)
• Jorge Cuellar (Principal Key Expert, Siemens)
• Christopher Oehmen (Lead and Chief Scientist of the Asymmetric Resilient Cybersecurity Initiative, Pacific Northwest National Lab)
• Greg Shannon (Asst Director for Cybersecurity Strategy, White House Office of Science & Technology)

Theory of Implementation Security (TIS 2016)
Monday, October 24, Lecture Hall I
PC Chairs: Begül Bilgin, Svetla Nikova, Vincent Rijmen (KU Leuven, Belgium)

07.30 – 09.00 Registration & Early-Bird Coffee

09.00 – 10.30 Welcome and Session 1
Session Chair: Vincent Rijmen (KU Leuven, Belgium)

Invited Talk: Masking and MPC: When Crypto Theory Meets Crypto Practice. Nigel Smart (University of Bristol)

Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order. Hannes Gross, Stefan Mangard, Thomas Korak (IAIK, Graz University of Technology)

10.30 – 11.00 Coffee Break

11.00 – 12.30 Session 2
Session Chair: Begül Bilgin (KU Leuven, Belgium)

Moments-Correlating DPA. Amir Moradi (Ruhr Universität Bochum), François-Xavier Standaert (Université catholique de Louvain)

Hiding Higher-Order Univariate Leaks by Shuffling Polynomial Masking Schemes. Fabrizio De Santis, Tobias Bauer and Georg Sigl (Technische Universität München)

12.30 – 14.00 Lunch Break

14.00 – 15.30 Session 3
Session Chair: Svetla Nikova (KU Leuven, Belgium)

Invited Talk: On Non-uniformity in Threshold Sharings. Joan Daemen (Radboud University Nijmegen and STMicroelectronics)

ParTI - Towards Combined Hardware Countermeasures against Side-Channel and Fault-Injection Attacks. Tobias Schneider, Amir Moradi, Tim Güneysu (Ruhr Universität Bochum)

15.30 – 16.00 Coffee Break

16.00 – 17.30 Session 4
Session Chair: Svetla Nikova (KU Leuven, Belgium)


Masking AES with d+1 Shares in Hardware. Thomas De Caudt, Oscar Reparaz, Bogil Bilgin, Svetla Nikova, Ventsislav Nikov, Vincent Rijmen (KU Leuven, NXP)

Monday, October 24, 2016
07.30 - 08.50 Registration & Early-Bird Coffee

08.50 - 10.30 Welcome and Session 1: Java Script
Session Chair: Deian Stefan (UC San Diego and Intrinsic)

Invited Talk: Flow: Analysis of JavaScript for type checking and beyond. Avik Chaudhuri (Facebook)


10.30 - 11.00 Coffee Break

11.00 - 12.30 Session 2: Information Flow
Session Chair: Tamara Reck (INRIA)

On Formalizing Information-Flow Control Libraries. Marco Vassena and Alejandro Russo (Chalmers University of Technology)

Future-dependent Flow Policies with Prophetic Variables. Ximeng Li, Flemming Nielson and Hanne Riis Nielson (Technical University of Denmark)

In-depth Enforcement of Dynamic Integrity Taint Analysis. Sepideh Amiri-Mohammadian and Christian Stahl (University of Vermont)

12.30 - 14.00 Lunch

14.00 - 15.30 Session 3: Program Analysis and Types
Session Chair: Marco Gaboardi (University at Buffalo)

JSPChecker: Static Detection of Context-Sensitive Cross-Site Scripting Flaws in Legacy Web Applications. Antonin Steinhauser (Oracle Labs) and Francois Gauthier (Charles University in Prague)

Rusty Types for Solid Safety (short paper). Sergio Benitez (Stanford University)

Bounding Information Leakage Using Implication Graph (short paper). Ziyuan Meng (Florida International University)

Dynamic Leakage - A Need for a New Quantitative Information Flow Measure (short paper). Nataliia Bizlova (INRIA)

15.30 - 16.00 Coffee Break

16.00 - 18.00 Session 4: Novel Applications
Session Chair: Toby Murray (University of Melbourne and Data61)

Invited Talk: Verified Secure Implementations for the HTTPS Ecosystem. Cedric Fournet (Microsoft Research)

Formal Verification of Smart Contracts. (short paper) Karthikkeyan Bhargavan (INRIA), Antoine Delignat-Lavaud, Cedric Fournet (Microsoft Research), Antilla Gollamudi (Harvard University), Georges Gonthier (Microsoft Research), Nadim Kobeissi (INRIA), Aseem Rastogi (Harvard University), Thomas Sibut-Pinette (INRIA), Nikhil Swamy and Santiago Zanella-Béguelin (Microsoft Research)

Automatic Trigger Generation for Rule-based Smart Homes. (short paper) Chandrakana Nandi and Michael D. Ernst (University of Washington)

Superhacks: Exploring and Preventing Vulnerabilities in Browser Binding Code. (short paper) Fraser Brown (Stanford University)

12.30 - 14.00 Lunch Break

07.30 - 09.00 Registration & Early Bird Coffee

09.00 - 10.30 Session 1: Cloud data security

Keynote: Data Analytics: Understanding Human Behavior Based on Mobile Network Data. Luciano Franceschini (Teralytics)

Co-Location Resistant Strategy with Full Resources Optimization. Berrima Moulsbe (University of Monastir)

10.30 - 11.00 Coffee Break

11.00 - 12.30 Session 2: Secure query processing, and web applications

Executing Boolean Queries on an Encrypted Bitmap Index. Mohamed Ahmed Abdelreheem, Christian Gehrmann, Lindström and Christian Nordahl (Swedish Institute of Computer Science)

Poly-Logarithmic Range Queries on Encrypted Data with Small Leakage. Florian Huhns and Florian Kerschbaum (SAP)

Encrypting Analytical Web Applications. Benny Fuhr, Walter Tighzert and Florian Kerschbaum (SAP Research)

12.30 - 14.00 Lunch Break

14.00 - 15.30 Session 3: Secure multitenancy & cloud attack detection

Keynote: Stratum Filtering: Cloud-based Detection of Attack Sources. Michael Waidner (Fraunhofer Institute for Secure Information Technology)

Oblivious RAM as a Substrate for Cloud Storage — The Leakage Challenge Ahead. Marc Sanchez-Artigas (Universitat Rovira i Virgili)

XAutomata: A Fast Policy Decision Process in Multi-Tenancy Cloud Environments. Meryem Ayache, Mohamed Eridi (ENSIAI, Mohammed V University), Ahmed Khousami and (University of Sherbrooke)

15.30 - 16.00 Coffee Break

16.00 - 18.00 Session 4: Secure storage and efficiency

On Information Leakage in Deduplicated Storage Systems. Hubert Ritzdorf (ETH Zurich, Switzerland), Ghassan Karam (NEC Laboratories Europe, Germany), Claudio Soriente (Telefonica, Spain) and Srifjan Capkun (ETH Zurich, Switzerland)

Message-Locked Proofs of Retrievability with Secure Deduplication. Dimitris Vasiliopoulos, Melek Onen, Kaouar Elkhayam and Refik Molva (EURECOM)

Generic Efficient Dynamic Proofs of Retrievability. Mohammad Etemad and Alpekin Kupcu (Koc University)

Assured Deletion in the Cloud: Requirements, Challenges and Future Directions. Kopo M. Ramachapan, Awaï Rashid and Jose M. Such (Lancaster University)

18.00 - 18.10 Closing
## 6th International Workshop on Trustworthy Embedded Devices (TrustED 2016)
**Friday, October 28, Lecture Hall F**
**PC Chairs: Xinxin Fan (Robert Bosch LLC, US), Tim Güneysu (University of Bremen & DFKI, DE)**

### 07.30 - 09.00 Registration & Early Bird Coffee

### 09.00 - 10.30 Session 1: Trusted Device Internals
**Session Chair: Tim Güneysu (University of Bremen & DFKI, DE)**

- **Keynote:** Analyzing Thousands of Firmware Images and a Few Physical Devices. What’s Next? 
  Aurelien Francillon (EURECOM, FR)

- **Side-channel attacks on fingerprint matching algorithms.** Markus Dürmuth (Ruhr-Universität Bochum, DE), David Oswald (University of Birmingham, UK) and Niklas Pastewka (Ruhr-Universität Bochum, DE)

### 10.30 - 11.00 Coffee Break

### 11.00 - 12.30 Session 2: Trusted Physical Entities
**Session Chair: Marcel Medwed (NXP, AT)**

- **Online Reliability Testing for PUF Key Derivation.** Matthias Hiller, Ayun Gurur Önal, Georg Sigl (Technical University of Munich, DE) and Martin Bossert (University of Ulm, DE)

- **Evaluation of Latch-based Physical Random Number Generator Implementation on 40nm ASICs.** Naoya Torii, Dai Yamamoto (FUJitsu Laboratories Ltd, JP) and Tsutomu Matsumoto (Yokohama National University, JP)

### 12.30 - 14.00 Lunch Break

---

## Second ACM Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC 2016)
**Friday, October 28, Lecture Hall E**
**PC Chairs: Rakesh Bobba (Oregon State University, USA), Alvaro Cardenas (University of Texas at Dallas, USA)**

### 07.30 - 08.50 Registration & Early Bird Coffee

### 08.50 - 10.30 Welcome and Session 1: Industrial Control Systems
**Session Chair: Michail Maniatakos (New York University, Abu Dhabi)**

**Automatic Construction of Statechart-Based Anomaly Detection Models for Multi-Threaded SCADA via Spectral Analysis.** Amit Kleinnmann and Avishai Wool (Tel-Aviv University)

**Towards High-Interaction Virtual ICS Honeypots-in-a-Box.** Daniele Antonioli, Anand Agrawal and Nils Ole Tippenhauer (Singapore University of Technology and Design)

**SENAMI: Selective Non-Invasive Active Monitoring for ICS Intrusion Detection.** William Jardine, Sylvin Frey, Benjamin Green and Awas Rashid (Lancaster University)

### 10.30 - 11.00 Coffee Break

### 11.00 - 12.30 Session 2: Vehicular CPS
**Session Chair: Pauline Anthonysamy (Google, Switzerland)**

**Secure Location Verification with a Mobile Receiver.** Richard Baker and Ivan Martinovic (University of Oxford)

**Risk Assessment for Cooperative Automated Driving.** Derrick Dominic (University of Michigan), Sameet Chhavri (UMTRI), Ryan Eaxte (University of Michigan), Di Ma (University of Michigan-Dearmont) and Andre Weimerskirch (University of Michigan)

**Towards Safe and Secure Autonomous and Cooperative Vehicle Ecosystems.** Antonio Lima, Francisco Rocha, Marcus Völpé and Paolo Estevess-Verissimo (University of Luxembourg)

### 12.30 - 14.00 Lunch Break

### 14.00 - 15.30 Session 3: Risk Assessment and Resilience
**Session Chair: Nils Ole Tippenhauer (Singapore University of Technology and Design)**

**Evaluating Resilience of Gas Pipeline Systems Under Cyber-Physical Attacks: A Function-Based Methodology.** Yatin Wadhawan (University of Southern California) and Clifford Neuman (Information Science Institute, USK)

**A Case Study on Implementing False Data Injection Attacks Against Nonlinear State Estimation.** Charalampos Konstantinou (New York University) and Michail Maniatakos (New York University, Abu Dhabi)

**Achieving ICS Resilience and Security through Granular Data Flow Management.** Benjamin Green (Lancaster University), Marina Krotofil (Honeywell Cyber Security Lab) and David Hutchison (Lancaster University)

### 15.30 - 16.00 Coffee Break

### 16.00 - 17.30 Session 4: Insights from Testbeds and Games
**Session Chair: Awas Rashid (Lancaster University, UK)**

**HAMIDS: An Hierarchical Monitoring Intrusion Detection System for Industrial Control Systems.** Hamid Reza Ghaemi and Nils Ole Tippenhauer (Singapore University of Technology and Design)

**SoftGrid: A Software-based Smart Grid Testbed for Evaluating Substation Cybersecurity Solutions.** Prageth Gunathilaka, Daisuke Mashima and Binbin Chen (Advanced Digital Sciences Center, Singapore)

**Exposing Transmitters in Mobile Multi-Agent Games.** Mai Ben Adar - Bessos (Bar - Ilan University), Simon Birnbach (University of Oxford), Amir Herzberg (Bar-Ilan University) and Ivan Martinovic (University of Oxford)

---

Friday, October 28, 2016
14.00 – 15.30 Session 3: V&V: Verification and model extraction of transformed software
Session Chair: Sakarno Mertorgano (Office of Naval Research)
Applications of Binary Analysis and Transformation in Security and Optimization. Joe Hendrix, Tristan Raveitch and Simon Winwood (Galois)
Safety-Security Control Code Verification. Saman Zonouz (Rutgers)
A Bottom-Up Verification Approach for Systems Software. Yakoob Nemouchi and Binoy Ravindran (Virginia Tech)
Open discussion led by session chair.

15.30 – 16.00 Coffee Break

16.00 – 18.00 Session 4: FET: Supporting and complementary approaches and methods for software transformation
Session Chair: Gary Toth (Office of Naval Research)
De-Inductive Reasoning and Explanation for Cybersecurity Threats (DIRECT). Anupam Datta (CMU), Matt Fredriksson (CMU), Joel Hylomega (UPenn), Andrew Myers (Cornell), Jonathan Smith (U Penn), Andrei Rierro (UPenn), Carolyn Talcott (SRI) and Nathan Dusenbahn (UPenn)
libdetox: A Framework for Online Program Transformation. Matthias Payer (Purdue)
ALLVM. Will Dietz and Vibrant Adve (UJIC)
Runtime Transformation through Augmented Binary Analysis. David Williams-King and Junfeng Yang (Columbia)
Open discussion led by session chair.

Open discussion led by session chair.

14.00 – 15.30 Session 3: Cyber Attacks & Network Security
Session Chair: Florian Kammuller (Middlesex University London and TU Berlin)
Cyber Deception: Virtual Networks to Defend Insider Reconnaissance. Stefan Achtenhein, Thomas La Porta, Patrick McDaniel (Pennsylvania State University, USA), Shridhar Sagar (Applied Communication Sciences, USA), Srikant Krishnamurthy (University of California, Riverside, USA) and Esha Chaudhary (Applied Communication Sciences, USA)
Pragmatic Security: Modelling IT Security Management Responsibilities for SME Archetypes. Simon Parkin (University College London, UK), Andrew Fielder (Imperial College London, UK) and Alex Ashby (Control Esc Ltd., Riverside, UK)
Ports Distribution Management for Privacy Protection inside Local Domain Name System. Fei Song, Wei Quan, Tianming Zhao, Hongke Zhang (Beijing Jiutong University, China), Ziwei Hu (Global Energy Interconnection Research Institute, China) and Ilsoon You (Soochunhyang University, Republic of Korea)

15.30 - 16.00 Coffee Break

16.00 - 17.30 Session 4 – short paper
Session Chair: Ilsoon You (Soochunhyang University, Republic of Korea)
Function-Based Access Control (FBAC): From Access Control Matrix to Access Control Tensor. Yoo Desmedt (The University of Texas at Dallas and University College London, USA) and Arash Shahghahi (The University of New South Wales (UNSW) and Data61, CSIRO, Australia)
WatchIT: Who Watches Your IT Guy? Noam Shalev, Idit Keidar (Technion, Israel), Yosef Moatti and Yaron Weinsberg (IBM Research, Israel)
A New Risk Assessment Framework Using Graph Theory for ICT complex systems. Mohamed Yassine Nacaouche, Sopho Pasero (Orange Labs, France), Radha Maljouba (LAMSAD, University Paris-Dauphine), Nizar Kheir and Jean-Philippe Wary (Orange Labs, France)
Online and offline security policy assessment. Fulvio Valenzia, Marco Vallini and Antonio Lioy (Politecnico di Torino, Italy)
A trippwire grammar for insider-threat detection. Ioannis Agrafiotis, Arman Erola, Michael Goldhamn and Sadie Creese (Oxford University, UK)
Discovering Insider Threats from Log Data with High-Performance Bioinformatics Tools. Markus Wurzemberger, Florian Skupik, Roman Fiedler (Austrian Institute of Technology, Austria) and Wolfgang Kastner (Vienna University of Technology, Austria)
Analysis on Manipulation of the MAC Address and Consequent Security Threats. Kyungroul Lee, Hyeyang Yun, Kangbin Yim (Soochunhyang University, Republic of Korea) and Sulhyun Kim (IT Security Research Center, Soochunhyang University, Republic of Korea)
Beyond the Attack Surface: Assessing Security
Introduction and Open Research Challenges.
08.30 – 09.30 Welcome and Session 1: Keynote
07.30 – 08.30 Registration & Early Bird Coffee
09.30 – 10.30 Session 2: Vulnerabilities
Session Chair: Jack Davidson (University of Virginia)
Beyond the Attack Surface: Assessing Security Risk with Random Walks on Call Graphs. Nathan Munisah and Andrew Mereoley (Rochester Institute of Technology)
ROP Gadget Prevalence and Survival under Compiler-based Binary Diversification Schemes. Joel Coffman, Daniel Kelly, Christopher Wellons and Andrew Gearhart (Johns Hopkins University Applied Physics Laboratory)
10.30 – 11.00 Coffee Break
11.00 – 12.30 Session 3: Obfuscation
Session Chair: Johannes Kinder (Royal Holloway, University of London)
Defeating MBA-based Obfuscation. Ninon Eyrolles (Quarkslab and LORIA)
VOT4CS: A Virtualization Obfuscation Tool for C#.. Sebastian Banescu, Ciprian Lucaci, Benjamin Knaer and Alexander Preitschmer (Technische Universität München)
Binary Permutation Polynomial Inversion and Application to Obfuscation Techniques. Lucas Barthélémy (Quarkslab and UPMC), Ninon Eyrolles (Quarkslab), Guenael Renault and Raphael Robin (UPMC).
12.00 – 14.00 Lunch Break
14.00 – 15.30 Session 4: White-box Crypto & Integrity
Session Chair: Christian Münch (Conax)
Stns4CS: A State Inspection Tool for C#. Amjad Ibraim and Sebastian Baneu (Technische Universität München)
Reactive Attestation: Automatic Detection and Reaction to Software Tampering Attacks. Alessio Viticchié (Politecnico di Torino), Andrea Avancini, Mariano Cecatto (Fondazione Bruno Kessler), Cataldo Basile (Politecnico di Torino), Bert Abrath and Bart Coppens (Ghent University)
Attacking White-Box AES Constructions. Brendan McMillion and Nick Sullivan (CloudFlare)
15.30 – 16.00 Coffee Break
16.00 – 18.00 Session 5: Panel Discussion
Session Chair: Brecht Wyseur (NAGRA, Switzerland)
Software Protection Research in Europe, where are we going?
16.30 – 18.00 Session 6: Hands-on Tutorial
The ASPIRE Framework for Software Protection. ASPIRE consortium
18.30 – 22.00 Dinner sponsored by NAGRA
08.50 – 10.00 Welcome and Keynote
Keynote: Why is applying machine learning to anti-abuse so hard? Elle Burststein (Google, Inc., US)
10.00 – 10.30 Session 1: Security Data Sets
Session Chair: David Mandell Freeman (LinkedIn Corporation, USA)
SherLock vs Moriarty: A Smartphone Dataset for Cybersecurity Research. Yorvel Mingky, Asaf Shahai, Lior Rochak, Bracha Shapira and Yuval Elovici (Ben-Gurion University, Israel)
10.30 – 11.00 Coffee Break
11.00 – 12.40 Session 2: Machine Learning and Security in Practice
Session Chair: Bastiaan Biggio (University of Cagliari, Italy)
Tracked Without a Trace: Linking Sessions of Users by Unsupervised Learning of Patterns in Their DNS Traffic. Matthias Kirchner (Humboldt University of Berlin, Germany), Dominik Herrmann, Jens Lindemann (University of Hamburg, Germany) and Marius Kloß (Humboldt University of Berlin, Germany)
Identifying Encrypted Malware Traffic with Contextual Flow Data. Blake Anderson and David McCrewe (Cisco Systems Inc., USA)
Causality-based Sensemaking of Network Traffic for Android Application Security. Hao Zhang, Danfeng Yao and Naren Ramakrishnan (Virginia Tech, USA)
12.40 – 14.15 Lunch Break
14.15 – 15.30 Session 3: Foundations
Session Chair: Brad Miller (Google, Inc., USA)
Secure Kernel Machines against Evasion Attacks. Paolo R assu, Ambra Demontis, Battista Biggio, Giorgio Fumera and Fabi o Roli (University of Cagliari, Italy)
Prescience: Probabilistic Guidance on the Retraining Conundrum for Malware Detection. Amit Des, Santanu Dash, Guillermo Suarez-Tangil, Vladimir Yor and Lorenzo Cavallaro (Royal Holloway, University of London, UK)
15.30 – 16.00 Coffee Break
16.00 – 17.40 Session 4: Privacy
Session Chair: Konrad Rieck (TU Braunschweig, Germany)
True Friends Let You Down: Benchmarking Social Graph Anonymization Schemes. Kumar Sharad (University of Cambridge, UK)
Change of Guard: The Next Generation of Social Graph De-anonymization Attacks. Kumar Sharad (University of Cambridge, UK)
Differentially Private Online Active Learning with Applications to Anomaly Detection. Motesh Ghasemi, Anand Sarwate and Rebecca Wright (Rutgers, The State University of New Jersey, USA)
A Dual Perturbation Approach for Differential Private ADMM-Based Distributed Empirical Risk Minimization. Tao Zhang and Qianyan Zhu (New York University, USA)
17.40 – 17.45 Conclusion
Friday, October 28, 2016
23rd ACM Conference on Computer and Communications Security
Hofburg Imperial Palace, Vienna, Austria, October 24-28, 2016
General Information

How to get from the city center to the airport

The Vienna International Airport (VIE) in Schwechat is about 20 km away in the southeast of Vienna. Train lines S7 and S2 (suburban railway “S-Bahn”), ICE/Railjet as well as the City Airport Train (CAT) connect the city center with the airport.

You can also take a taxi for your convenience, a taxi fare is at about 30 Euro. We recommend a pre-booked taxi with airportdriver.at. It can be booked online: http://www.airportdriver.at/enairport-transfer.

Overview about connections

<table>
<thead>
<tr>
<th>Connections</th>
<th>CAT</th>
<th>S-Bahn</th>
<th>ICE / Railjet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Price</td>
<td>11 €</td>
<td>3,9 €</td>
<td>3,9 €</td>
</tr>
<tr>
<td>Duration</td>
<td>16 min</td>
<td>25 min</td>
<td>18 min</td>
</tr>
</tbody>
</table>

The closest underground stops

- U2 “Herrenngasse” exit: “Fahnengasse”
- U3 “Stephansplatz” exit: “Graben”
- U2 “Volkstheater” exit “Dr. Karl Renner Ring”

conferenc venue

Hofburg Imperial Palace Vienna
Congress Center Hofburg
Entrance Botschafterstiege – Schweizerhof
1010 Vienna

GPS Coordinates: 48.206843, 16.365629
The closest underground stops:

- U3 "Herrengasse" exit: "Fahnengasse"
- U1 / U3 "Stephansplatz" exit: "Graben"
- U2 "Volkstheater" exit "Dr. Karl Renner Ring"
### ACM CCS 2016

#### Tuesday, October 25, 2016

<table>
<thead>
<tr>
<th>Track 1</th>
<th>Track 2</th>
<th>Track 3</th>
<th>Track 4</th>
<th>Track 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>LH A</td>
<td>LH B</td>
<td>LH C</td>
<td>LH D</td>
<td>LH E</td>
</tr>
<tr>
<td>07:30</td>
<td>08:40</td>
<td>08:50</td>
<td>10:00</td>
<td>10:30</td>
</tr>
</tbody>
</table>
| Registration & Early Bird Coffee | Keynote @ LH C  
Cybersecurity, Nuclear Security, Alan Turing, and Illogical Logic  
Martin Hellman (Stanford University, US) | Session 1A | Session 1B | Session 1C | Session 1D | Tutorial 1 |
| 11:30   | 12:00   | 12:00   | 13:00   | 13:00   |
| Coffee Break | Lunch Break | Session 2A | Session 2B | Session 2C | Session 2D | Invited Talk |
| 14:30   | 15:00   | 15:00   | 16:00   | 16:00   |
| Session 3A | Session 3B | Session 3C | Session 3D | Tutorial 2 |
| 16:00   | 16:30   | 16:30   | 18:00   | 18:00   |
| Coffee Break | Coffee Break | Session 4A | Session 4B | Session 4C | Session 4D | Tutorial 2 |
| 18:30   | 19:00   | 19:00   | 19:00   | 23:00   |
| Mayor's Dinner @ Vienna City Hall | Poster / Demo Session & Award Ceremony |

#### Wednesday, October 26, 2016

<table>
<thead>
<tr>
<th>Track 1</th>
<th>Track 2</th>
<th>Track 3</th>
<th>Track 4</th>
<th>Track 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>LH A</td>
<td>LH B</td>
<td>LH C</td>
<td>LH D</td>
<td>LH E</td>
</tr>
<tr>
<td>07:30</td>
<td>08:40</td>
<td>08:50</td>
<td>10:00</td>
<td>10:30</td>
</tr>
</tbody>
</table>
| Registration & Early Bird Coffee | Is it practical to build a truly distributed payment system?  
Ross Anderson (University of Cambridge, UK) | Session 5A | Session 5B | Session 5C | Session 5D | Tutorial 3 |
| 11:30   | 12:00   | 12:00   | 13:00   | 13:00   |
| Coffee Break | Lunch Break | Session 6A | Session 6B | Session 6C | Session 6D | Tutorial 4 12:00-13:15 |
| 14:30   | 15:00   | 15:00   | 16:00   | 16:00   |
| Session 7A | Session 7B | Session 7C | Session 7D | Session 7E |
| 16:00   | 16:30   | 16:30   | 18:00   | 18:00   |
| Coffee Break | Coffee Break | Session 8A | Session 8B | Session 8C | Session 8D | Invited Talks |
| 18:05   | 19:00   | 19:00   | 19:00   | 24:00   |
| Panel Discussion @ LH C  
Impact of Academic Security Research: Frogs in Wells, Storms in Teacups, or Raw Diamonds? | Traditional Viennese Dinner @ Heuriger |

#### Thursday, October 27, 2016

<table>
<thead>
<tr>
<th>Track 1</th>
<th>Track 2</th>
<th>Track 3</th>
<th>Track 4</th>
<th>Track 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>LH A</td>
<td>LH B</td>
<td>LH C</td>
<td>LH D</td>
<td>LH E</td>
</tr>
<tr>
<td>08:15</td>
<td>09:30</td>
<td>09:30</td>
<td>11:00</td>
<td>11:00</td>
</tr>
<tr>
<td>Registration &amp; Early Bird Coffee</td>
<td>Coffee Break</td>
<td>Session 9A</td>
<td>Session 9B</td>
<td>Session 9C</td>
</tr>
<tr>
<td>11:30</td>
<td>11:30</td>
<td>11:30</td>
<td>13:00</td>
<td>13:00</td>
</tr>
<tr>
<td>Lunch Break</td>
<td>Lunch Break</td>
<td>Session 10A</td>
<td>Session 10B</td>
<td>Session 10C</td>
</tr>
<tr>
<td>14:30</td>
<td>14:30</td>
<td>14:30</td>
<td>16:00</td>
<td>16:00</td>
</tr>
<tr>
<td>Session 11A</td>
<td>Session 11B</td>
<td>Session 11C</td>
<td>Session 11D</td>
<td>Session 11E</td>
</tr>
<tr>
<td>16:00</td>
<td>16:30</td>
<td>16:30</td>
<td>18:00</td>
<td>18:00</td>
</tr>
<tr>
<td>Coffee Break</td>
<td>Coffee Break</td>
<td>Session 12A</td>
<td>Session 12B</td>
<td>Session 12C</td>
</tr>
<tr>
<td>18:05</td>
<td>19:00</td>
<td>19:00</td>
<td>19:00</td>
<td>20:45</td>
</tr>
</tbody>
</table>
| CCS Business Meeting @ LH C | Sightseeing  
For ticket holders only! (Window for purchase closed on 21/10/2016) |

#### SHORT INDEX

- Keynotes / Invited Industrial Talks / Tutorial / Panel: p.4-10
- Agenda CCS Main Conference: p.11-19
- Posters / Demos: p.20
- Agenda Pre- & Post-Workshops: p.21-27
- Floor plans: p.28-29
- schedule

@acm_ccs #ccs16
ssid: CCS_Participants
pwd: cc4s3curity

23rd ACM Conference on Computer and Communications Security  
Hofburg Imperial Palace, Vienna, Austria, October 24-28, 2016