

ACM CCS 2016

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

[Program Guide](#)



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)



Shai Halevi
(IBM Research, 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)



Aniket Kate
(Purdue University, USA)

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)



Giovanni Livraga
(Università degli Studi di Milano, Italy)

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
(George Washington University, USA)



Giovanni Vigna
(University of California, Santa Barbara, USA)



George Danezis
(University College London, UK)



Trent Jaeger (SIGSAC Chair)
(Pennsylvania State University, US)



Stefan Savage
(University of California, San Diego, US)



David Basin
(ETH Zurich, Switzerland)

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 keynotes 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.



Martin Hellman
Stanford University, USA
ACM A.M. Turing Award Winner 2015

Cybersecurity, Nuclear Security, Alan Turing, and Illogical 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 one of the first two dozen "Stanford Engineering Heroes," the National Inventors Hall of Fame, and the Marconi International Fellowship – and,

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.



Ross Anderson
University of Cambridge, UK

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 prepayment 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 built 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

**Timo Kasper***Kasper&Oswald GmbH, Germany*

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).

**Thorsten Borrman***DB Netz AG, Germany*

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 Borrman 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.

Tuesday, October 25, 2016, 12.00-13.00, Lecture Hall E

Wednesday, October 26, 2016, 16.30-17.15, Lecture Hall E



Klaus Kursawe
GridSec.org, The Netherlands

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 unending 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.



Xiaokui Shu
IBM T. J. Watson
Research Center, USA

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.



Danfeng Yao
Department of Computer Science
Virginia Tech, USA

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 current 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



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.

[20] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. *Sok: Research perspectives and challenges for bitcoin and cryptocurrencies*. In *IEEE Symposium on Security and Privacy*, 2015.5, 2016

Aljoshia Judmayer received a master's degree in Software Engineering and Internet Computing at the Vienna University of Technology. He has several years of experience in penetration testing as IT security consultant. At the moment, he is working as IT security researcher at SBA Research, where he is also working towards his Ph.D. degree on applications of cryptographic currencies and resilience aspects of distributed systems. His research interests include network security, applied cryptography and cryptographic currencies.

**Aniket Kate***Purdue University, USA*

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 to fix apparent flaws have made 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.

**Ghassan O. Karame***NEC Laboratories Europe, Germany*

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.

Wednesday, October 26, 2016, 12.00-13.15, Lecture Hall E - Tutorial 4

Wednesday, October 26, 2016, 14.30-16.00, Lecture Hall E - Tutorial 5



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).



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.



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).



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.



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.



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.

Wednesday, October 26, 2016, 18.00 - 19.00, Lecture Hall C



CCS 2016 Main Conference, Tuesday, October 25, 2016

	Track 1 Cryptographic Mechanisms Lecture Hall A	Track 2 Differential Privacy / Cryptography / Attacks Lecture Hall B	Track 3 Web/Mobile Security Lecture Hall C	Track 4 Secure Code and Systems Lecture Hall D	Track 5 Tutorials & Talks Lecture Hall E
07.30 08.40	Registration & Early Bird Coffee				
08.40 08.50	Opening - Lecture Hall C				
08.50 09.50	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	Session 1A Blockchain I Ian Goldberg (University of Waterloo)	Session 1B Differential Privacy Prateek Mittal (Princeton University)	Session 1C Android Security XiaoFeng Wang (Indiana University)	Session 1D Hardware Protection Taesoo Kim (Georgia Tech)	Tutorial 1
	On the Security and Performance of Proof of Work Blockchains <i>Arthur Gervais (ETH Zürich), Ghassan O. Karame (NEC Laboratories Europe), Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf and Srdjan Capkun (ETH Zürich)</i>	Differential Privacy as a Mutual Information Constraint <i>Paul Cuff and Langqin Yu (Princeton University)</i>	The Misuse of Android Unix Domain Sockets and Security Implications <i>Yuru Shao (University of Michigan), Jason Ott (University of California, Riverside), Yunhan Jack Jia (University of Michigan), Zhiyun Qian (University of California, Riverside) and Z. Morley Mao (University of Michigan)</i>	Strong Non-Interference and Type-Directed Higher-Order Masking <i>Gilles Barthe (IMDEA Software Institute), Sonia Belaïd (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)</i>	Program Anomaly Detection: Methodology and Practices <i>Xiaokui Shu (IBM T. J. Watson Research Center, USA) & Danfeng Yao (Department of Computer Science Virginia Tech, USA)</i>
	A Secure Sharding Protocol For Open Blockchains <i>Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert and Prateek Saxena (National University of Singapore)</i>	Advanced Probabilistic Couplings for Differential Privacy <i>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)</i>	Call Me Back! Attacks on System Server and System Apps in Android through Synchronous Callback <i>Kai Wang, Yuqing Zhang (University of Chinese Academy of Sciences, Beijing) and Peng Liu (The Pennsylvania State University)</i>	MERS: Statistical Test Generation for Side - Channel Analysis based Trojan Detection <i>Yuanwen Huang, Swarup Bhunia and Prabhat Mishra (University of Florida)</i>	
	The Honey Badger of BFT Protocols <i>Andrew Miller (University of Maryland), Yu Xia (Tsinghua University), Kyle Croman, Elaine Shi (Cornell University) and Dawn Song (University of California)</i>	Differentially Private Bayesian Programming <i>Gilles Barthe (IMDEA Software Institute), Gian Pietro Farina, 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)</i>	Draco: A System for Uniform and Fine-grained Access Control for Web Code on Android <i>Guliz Seray Tuncay, Soteris Demetriou and Carl A. Gunter (University of Illinois at Urbana - Champaign)</i>	Private Circuits III: Hardware Trojan-Resilience via Testing Amplification <i>Stefan Dziembowski (University of Warsaw), Sebastian Faust (University of Bochum) and Francois - Xavier Standaert (Université catholique de Louvain)</i>	
11.30 12.00	Coffee Break				

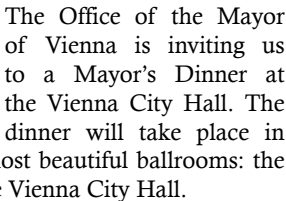


CCS 2016 Main Conference, Tuesday, October 25, 2016

	Track 1 Cryptographic Mechanisms Lecture Hall A	Track 2 Differential Privacy / Cryptography / Attacks Lecture Hall B	Track 3 Web/Mobile Security Lecture Hall C	Track 4 Secure Code and Systems Lecture Hall D	Track 5 Tutorials & Talks Lecture Hall E
12.00 13.00	Session 2A Blockchain II Edgar Weippl (SBA Research)	Session 2B Differentially Private Systems I Shai Halevi (IBM Research)	Session 2C Access Control Gail-Joon Ahn (Arizona State University)	Session 2D Security and Persistence William Robertson (Northeastern University)	Invited Industrial Talk
	On the Instability of Bitcoin Without the Block Reward <i>Miles Carlsten, Harry Kalodner, S. Matthew Weinberg and Arvind Narayanan (Princeton University)</i>	A EpicRec: Towards Practical Differentially Private Framework for Personalized Recommendation <i>Yilin Shen and Hongxia Jin (Samsung Research America)</i>	AUDACIOUS: User-Driven Access Control with Unmodified Operating Systems <i>Talia Ringer, Dan Grossman and Franziska Roesner (University of Washington)</i>	Safe Serializable Secure Scheduling: Transactions and the Trade - Off Between Security and Consistency <i>Isaac Sheff, Tom Magrino, Jed Liu, Andrew C. Myers and Robert Van Renesse (Cornell)</i>	Colorful like a Chameleon: Security Nightmares of Embedded Systems <i>Timo Kasper (Kasper&Oswald GmbH, Germany)</i>
	Transparency Overlays and Applications <i>Melissa Chase (Microsoft Research Redmond) and Sarah Meiklejohn (University College London)</i>	Heavy Hitter Estimation over Set - Valued Data with Local Differential Privacy <i>Zhan Qin (Qatar Computing Research Institute), Yin Yang (Hamad Bin Khalifa University), Ting Yu, Issa Khalil (Qatar Computing Research Institute), Xiaokui Xiao (Nanyang Technological University) and Kui Ren (SUNY Buffalo)</i>	Mix&Slice: Efficient Access Revocation in the Cloud <i>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)</i>	ProvUSB: Block - level Provenance - Based Data Protection for USB Storage Devices <i>Dave (Jing) Tian (University of Florida), Adam Bates (University of Illinois at Urbana - Champaign), Kevin R.B. Butler (University of Florida) and Raju Rangaswami (Florida International University)</i>	
13.00 14.30	Lunch Break				
14.30 16.00	Session 3A Smart Contracts Sarah Meiklejohn (University College London)	Session 3B Differentially Private Systems II Ting Yu (Qatar Computing Research Institute)	Session 3C Mobile Software Analysis Will Enck (NC State University)	Session 3D Kernel Memory Security Herbert Bos (Vrije Universiteit)	Tutorial 2
	Making Smart Contracts Smarter <i>Loi Luu, Duc - Hiep Chu (National University of Singapore), Hrishi Olickel (Yale - NUS College), Prateek Saxena (National University of Singapore) and Aquinas Hobor (Yale - NUS College & National University of Singapore)</i>	DPSense: Differentially Private Crowdsourced Spectrum Sensing <i>Xiaocong Jin (Arizona State University), Rui Zhang (University of Hawaii), Yimin Chen, Tao Li and Yanchao Zhang (Arizona State University)</i>	TaintART: A Practical Multi-level Information - Flow Tracking System for Android RunTime <i>Mingshen Sun (The Chinese University of Hong Kong), Tao Wei (Baidu) and John C.S. Lui (The Chinese University of Hong Kong)</i>	Prefetch Side-Channel Attacks: Bypassing SMAP and Kernel ASLR <i>Daniel Gruss, Clémentine Maurice (TU Graz), Andreas Fogh (G - Data Advanced Analytics), Moritz Lipp and Stefan Mangard (TU Graz)</i>	Security on Wheels: Security and Privacy for Vehicular Communication Systems - Part I <i>Panos Papadimitratos (KTH, Sweden)</i>
	Town Crier: An Authenticated Data Feed for Smart Contracts <i>Fan Zhang, Ethan Cecchetti (Cornell University), Kyle Croman (Jacobs Institute), Ari Juels (Cornell Tech) and Elaine Shi (Cornell University)</i>	Deep Learning with Differential Privacy <i>Martin Abadi, Andy Chu (Google), Ian Goodfellow (OpenAI), H. Brendan McMahan, Ilya Mironov, Kunal Talwar and Li Zhang (Google)</i>	Statistical Deobfuscation of Android Applications <i>Benjamin Bichsel, Veselin Raychev, Petar Tsankov and Martin Vechev (ETH Zurich)</i>	Breaking Kernel Address Space Layout Randomization with Intel TSX <i>Yeongjin Jang, Sangho Lee and Taesoo Kim (Georgia Institute of Technology)</i>	
	The Ring of Gyges: Investigating the Future of Criminal Smart Contracts <i>Ari Juels (Jacobs Institute), Ahmed Kosba (University of Maryland) and Elaine Shi (Cornell University)</i>	Membership Privacy in MicroRNA - based Studies <i>Michael Backes, Pascal Berrang, Mathias Humbert and Praveen Manoharan (CISPA)</i>	Reliable Third - Party Library Detection in Android and its Security Applications <i>Michael Backes, Sven Bugiel and Erik Derr (CISPA, Saarland University)</i>	Enforcing Least Privilege Memory Views for Multithreaded Applications <i>Terry Ching - Hsiang Hsu (Purdue University), Kevin Hoffman (eFolder), Patrick Eugster (TU Darmstadt) and Mathias Payer (Purdue University)</i>	
16.00 16.30	Coffee Break				

$$\begin{array}{r} 18.30 \\ - 23.00 \\ \hline \end{array}$$

Tuesday, October 25, 2016 | 18.30 – 23.00



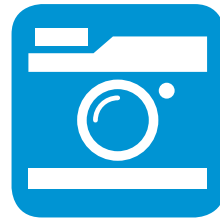
Agenda:

- How to get there:*

[illegible]

CCS 2016 Main Conference, Wednesday, October 26, 2016

	Track 1 Cryptographic Mechanisms Lecture Hall A	Track 2 Differential Privacy / Cryptography / Attacks Lecture Hall B	Track 3 Web/Mobile Security Lecture Hall C	Track 4 Secure Code and Systems Lecture Hall D	Track 5 Tutorials & Talks Lecture Hall E
07.30 08.50	Registration & Early Bird Coffee				
08.50 09.50	Keynote Is it practical to build a truly distributed payment system? Keynote by Ross Anderson, University of Cambridge, UK Lecture Hall C				
10.00 11.30	Session 5A Secure MPC II Claudio Orlandi (Aarhus University)	Session 5B Physically Based Authentication Erman Ayday (Bilkent University)	Session 5C Web Security Ben Livshits (Microsoft Research)	Session 5D Security Bug Finding Adam Doupé (Arizona State University)	Tutorial 3
	Alternative Implementations of Secure Real Numbers <i>Vassil Dimitrov (University of Calgary), Liisi Kerik (Cybernetica), Toomas Krips (STACC), Jaak Randmets and Jan Willemson (Cybernetica)</i>	MEMS Gyroscopes as Physical Uncloable Functions <i>Oliver Willers, Christopher Huth (Robert Bosch GmbH), Jorge Guajardo (Robert Bosch LLC – RTC) and Helmut Seidel (Saarland University)</i>	Measurement and Analysis of Private Key Sharing in the HTTPS Ecosystem <i>Frank Cangialosi (University of Maryland), Taejoong Chung, David Choffnes (Northeastern University), Dave Levin (University of Maryland), Bruce M. Maggs (Duke University), Alan Mislove and Christo Wilson (Northeastern University)</i>	How I Learned to be Secure: a Census - Representative Survey of Security Advice Sources and Behavior <i>Elissa M. Redmiles (University of Maryland), Sean Kross (Johns Hopkins University) and Michelle L. Mazurek (University of Maryland)</i>	(CCS)^2 – Crypto - Currencies Special @ CCS 2016 (Part I) Cryptographic Currencies Crash Course (C5) <i>Aljosha Judmayer (SBA Research, Austria)</i>
	Garbling Gadgets for Boolean and Arithmetic Circuits <i>Marshall Ball, Tal Malkin (Columbia University) and Mike Rosulek (Oregon State University)</i>	On the Security and Usability of Segment - based Visual Cryptographic Authentication Protocols <i>Tianhao Wang, Huangyi Ge, Omar Chowdhury, Hemanta K. Maij and Ninghui Li (Purdue University)</i>	Chainsaw: Chained Automated Workflow - based Exploit Generation <i>Abeer Alhuzali, Birhanu Eshete, Rigel Gjomemo and V.N. Venkatakrishnan (University of Illinois at Chicago)</i>	Practical Detection of Entropy Loss in Pseudo - Random Number Generators <i>Felix Dörre and Vladimir Klebanov (Karlsruhe Institute of Technology)</i>	
	Optimizing Semi - Honest Secure Multiparty Computation for the Internet <i>Aner Ben - Efraim (Ben - Gurion University), Yehuda Lindell (Bar - Ilan University) and Eran Omri (Ariel University)</i>	Instant and Robust Authentication and Key Agreement among Mobile Devices <i>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)</i>	CSPAutoGen: Black-box Enforcement of Content Security Policy upon Real-world Websites <i>Xiang Pan (Northwestern University), Yinzhi Cao (Lehigh University), Shuangping Liu, Yu Zhou, Yan Chen, Yang Hu (Northwestern University) and Tingzhe Zhou (Lehigh University)</i>	Build It, Break It, Fix It: Contesting Secure Development <i>Andrew Ruef, Michael Hicks, James Parker, Dave Levin, Michelle L. Mazurek (University of Maryland) and Piotr Mardziel (Carnegie Mellon University)</i>	
11.30 12.00	Coffee Break				




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.

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

CCS 2016 Main Conference, Wednesday, October 26, 2016

	Track 1 Cryptographic Mechanisms Lecture Hall A	Track 2 Differential Privacy / Cryptography / Attacks Lecture Hall B	Track 3 Web/Mobile Security Lecture Hall C	Track 4 Secure Code and Systems Lecture Hall D	Track 5 Tutorials & Talks Lecture Hall E
16.00 16.30	Coffee Break				
16.30 18.00	Session 8A Lattices and Obfuscation Stefan Dziembowski (University of Warsaw)	Session 8B Attacks and Defences Yinqian Zhang (The Ohio State University)	Session 8C Phone Security Manuel Egele (Boston University)	Session 8D Infrastructure Attacks Zhiyun Qian (UC Riverside)	Invited Industrial Talks
	5Gen: A Framework for Prototyping Applications Using Multilinear Maps and Matrix Branching Programs <i>Kevin Lewi (Stanford University), Alex J. Malozemoff (Galois), Daniel Apon (University of Maryland), Brent Carmer (Oregon State University), Adam Foltzer, Daniel Wagner, David W. Archer (Galois), Dan Boneh (Stanford University), Jonathan Katz (University of Maryland) and Mariana Raykova (Yale University)</i>	On Code Execution Tracking via Power Side - Channel <i>Yannan Liu, Lingxiao Wei, Zhe Zhou, Kehuan Zhang (The Chinese University of Hong Kong), Wenyuan Xu (Zhejiang University) and Qiang Xu (The Chinese University of Hong Kong)</i>	Using Reflexive Eye Movements For Fast Challenge - Response Authentication <i>Ivo Sluganovic, Marc Roeschlin, Kasper B. Rasmussen and Ivan Martinovic (University of Oxford)</i>	Limiting the Impact of Stealthy Attacks on Industrial Control Systems <i>David I. Urbina, Jairo Giraldo, Alvaro A. Cardenas (The University of Texas at Dallas), Nils Ole Tippenhauer (Singapore University of Technology and Design), Junia Valente, Mustafa Faisal, Justin Ruths (The University of Texas at Dallas), Richard Candell (National Institute of Standards and Technology) and Henrik Sandberg (Royal Institute of Technology)</i>	Design requirements on resilient command control and signaling systems in the railway sector – first preliminary results of the CYSIS working group on IT security <i>Thorsten Borrmann (DB Netz AG, Germany) (16.30 – 17.15)</i>
	Λoλ: Functional Lattice Cryptography <i>Eric Crockett (Georgia Institute of Technology) and Chris Peikert (University of Michigan)</i>	Drammer: Deterministic Rowhammer Attacks on Mobile Platforms <i>Victor van der Veen (Vrije Universiteit Amsterdam), Yanick Fratantonio, Martina Lindorfer (UC Santa Barbara), Daniel Gruss, Clementine Maurice (TU Graz), Giovanni Vigna (UC Santa Barbara), Herbert Bos, Kaveh Razavi and Cristiano Giuffrida (Vrije Universiteit Amsterdam)</i>	When CSI Meets Public WiFi: Inferring Your Mobile Phone Password via WiFi Signals <i>Mengyuan Li, Yan Meng, Junyi Liu, Haojin Zhu (Shanghai Jiao Tong University), Xiaohui Liang (University of Massachusetts at Boston), Yao Liu (University of South Florida) and Na Ruan (Shanghai Jiao Tong University)</i>	Over - The - Top Bypass: Study of a Recent Telephony Fraud <i>Merve Sahin and Aurélien Francillon (Eurecom)</i>	Experiences in Securing Smart Grids and their Operations <i>Klaus Kursawe (GridSec.org, The Netherlands) (17.15 – 18.00)</i>
	Frodo: Take off the ring! Practical, Quantum - Secure Key Exchange from LWE <i>Joppe Bos (NXP Semiconductors), Craig Costello (Microsoft Research), Léo Ducas (CWI), Ilya Mironov (Google), Michael Naehrig (Microsoft Research), Valeria Nikolaenko (Stanford University), Ananth Raghunathan (Google) and Douglas Stebila (McMaster University)</i>	Error Handling of In - vehicle Networks Makes Them Vulnerable <i>Kyong - Tak Cho and Kang G. Shin (University of Michigan)</i>	VoicELive: A Phoneme Localization based Liveness Detection for Voice Authentication on Smartphones <i>Linghan Zhang, Sheng Tan, Jie Yang (Florida State University) and Yingying Chen (Stevens Institute of Technology)</i>	New Security Threats Caused by IMS - based SMS Service in 4G LTE Networks <i>Guan - Hua Tu (Michigan State University), Chi - Yu Li (National Chiao Tung University), Chunyi Peng (Ohio State University), Yuanjie Li and Songwu Lu (University of California, Los Angeles)</i>	
18.05 19.00	Panel Discussion Impact of Academic Security Research: Frogs in Wells, Storms in Teacups, or Raw Diamonds? Chair: Ahmad - Reza Sadeghi, TU Darmstadt, CYSEC, 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				
19.05 24.00	Traditional Viennese Dinner @ Heuriger <i>„Man bringe den Spritzwein!“ aka “Get me the sparkling wine!”</i> <i>(Quote: Michael Häupl, Mayor of the City of Vienna)</i> 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. 19.05 Meeting point in front of the Conference Venue entrance 19.10 Departure of the busses (20min drive) 22.00 – 24.00 Busses at regular intervals back to the Conference Venue				



CCS 2016 Main Conference, Thursday, October 27, 2016

	Track 1 Cryptographic Mechanisms Lecture Hall A	Track 2 Differential Privacy / Cryptography / Attacks Lecture Hall B	Track 3 Web/Mobile security Lecture Hall C	Track 4 Secure Code and Systems Lecture Hall D	Track 5 Tutorials & Talks Lecture Hall E
08.15 09.30	Registration & Early-Bird Coffee				
09.00 09.30 11.00	Session 9A Order-Revealing and Searchable Encryption (09.00 – 11.00) Florian Kerschbaum (SAP SE)	Session 9B Authentication (09.30 – 11.00) Frederik Armknecht (University of Mannheim)	Session 9C Passwords (09.30 – 11.00) Wenyuan Xu (University of South Carolina)	Session 9D Internet Security (09.30 – 11.00) Konrad Rieck (TU Braunschweig)	
	POPE: Partial Order Preserving Encoding <i>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)</i>	Practical Anonymous Password Authentication and TLS with Anonymous Client Authentication <i>Zhenfeng Zhang, Kang Yang (Chinese Academy of Sciences), Xuexian Hu (State Key Laboratory of Mathematical Engineering and Advanced Computing) and Yuchen Wang (Chinese Academy of Sciences)</i>	An Empirical Study of Mnemonic Sentence-based Password Generation Strategies <i>Weining Yang, Ninghui Li, Omar Chowdhury, Aiping Xiong and Robert W. Proctor (Purdue University)</i>	PIPSEA: A Practical IPsec Gateway on Embedded APUs <i>Jungho Park, Wookeun Jung, Gangwon Jo, Ilkoo Lee and Jaemin Lee (Seoul National University)</i>	
	Σοφός – Forward Secure Searchable Encryption <i>Raphael Bost (Direction Générale de l'Armement – Maitrise de l'Information & Université de Rennes 1)</i>	Efficient Cryptographic Password Hardening Services From Partially Oblivious Commitments <i>Jonas Schneider, Nils Fleischhacker (CISPA, Saarland University), Dominique Schröder (Friedrich-Alexander-University Erlangen-Nürnberg) and Michael Backes (Saarland University)</i>	On the Security of Cracking-Resistant Password Vaults <i>Maximilian Golla, Benedict Beuscher and Markus Dürmuth (Ruhr-University Bochum)</i>	MiddlePolice: Toward Enforcing Destination-Defined Policies in the Middle of the Internet <i>Zhuotao Liu (UIUC), Hao Jin (Nanjing University), Yih-Chun Hu and Michael Bailey (UIUC)</i>	
	What Else is Revealed by Order-Revealing Encryption? <i>F. Betül Durak (Rutgers University), Thomas M. DuBuisson (Galois) and David Cash (Rutgers University)</i>	A Comprehensive Formal Security Analysis of OAuth 2.0 <i>Daniel Fett, Ralf Küsters and Guido Schmitz (University of Trier)</i>	Targeted Online Password Guessing: An Underestimated Threat <i>Ding Wang, Zijian Zhang, Ping Wang (Peking University), Jeff Yan (Lancaster University) and Xinyi Huang (Fujian Normal University)</i>	Protecting Insecure Communications with Topology-aware Network Tunnels <i>Georgios Kontaxis and Angelos D. Keromytis (Columbia University)</i>	
	Order-Revealing Encryption: New Constructions, Applications, and Lower Bounds <i>Kevin Lewi and David J. Wu (Stanford University)</i>				
11.00 11.30	Coffee Break				



CCS 2016 Main Conference, Thursday, October 27, 2016

	Track 1 Cryptographic Mechanisms Lecture Hall A	Track 2 Differential Privacy / Cryptography / Attacks Lecture Hall B	Track 3 Web/Mobile Security Lecture Hall C	Track 4 Secure Code and Systems Lecture Hall D	Track 5 Tutorials & Talks Lecture Hall E
11.30 13.00	Session 10A Specialized Crypto Tools Abhi Shelat (Northeastern University)	Session 10B Crypto Implementations Jakub Szefer (Yale University)	Session 10C Measuring Security in the Wild Alejandro Russo (Chalmers Univ. of Technology)	Session 10D Network Security I Mohammad Mannan (Concordia University)	Tutorial 6
	Function Secret Sharing: Improvements and Extensions <i>Elette Boyle (IDC Herzliya), Niv Gilboa (Ben Gurion University) and Yuval Ishai (Technion)</i>	A Surfeit of SSH Cipher Suites <i>Maritin R. Albrecht, Jean Paul Degabriele, Torben Brandt Hansen and Kenneth G. Paterson (Royal Holloway, University of London)</i>	Content Security Problems? Evaluating the Effectiveness of Content Security Policy in the Wild <i>Stefano Calzavara, Alvise Rabitti and Michele Bugliesi (Università Ca' Foscari Venezia)</i>	PhishEye: Live Monitoring of Sandboxed Phishing Kits <i>Xiao Han, Nizar Kheir (Orange Labs) and Davide Balzarotti (Eurecom)</i>	Privacy and Security in the Genomic Era <i>Erman Ayday (Bilkent University, Turkey) & Jean-Pierre Hubaux (EPFL, Switzerland)</i>
	Hash First, Argue Later: Adaptive Verifiable Computations on Outsourced Data <i>Dario Fiore (IMDEA Software Institute), Cédric Fournet (Microsoft Research), Esha Ghosh (Brown University), Markulf Kohlweiss, Olga Ohrimenko and Bryan Parno (Microsoft Research)</i>	Systematic Fuzzing and Testing of TLS Libraries <i>Juraj Somorovsky (Ruhr University Bochum)</i>	CSP is Dead, Long Live CSP! On the Insecurity of Whitelists and the Future of the Content Security Policy <i>Lukas Weichselbaum, Michele Spagnuolo, Sebastian Lekies and Artur Janc (Google)</i>	All Your DNS Records Point to Us: Understanding the Security Threats of Dangling DNS Records <i>Daiping Liu (University of Delaware), Shuai Hao College of (William and Mary) and Haining Wang (University of Delaware)</i>	
	Practical Non-Malleable Codes from I-more Extractable Hash Functions <i>Aggelos Kiayias (University of Edinburgh), Feng-Hao Liu (Florida Atlantic University) and Yiannis Tselekounis (University of Athens)</i>	Attacking OpenSSL Implementation of ECDSA with a Few Signatures <i>Shuqin Fan (State Key Laboratory of Cryptology), Wenbo Wang and Qingfeng Cheng (Luoyang University of Foreign Languages)</i>	Online tracking: A 1-million-site measurement and analysis <i>Steven Englehardt and Arvind Narayanan (Princeton University)</i>	Identifying the Scan and Attack Infrastructure Behind Amplification DDoS Attacks <i>Johannes Krupp, Michael Backes and Chirstian Rossow (CISPA, Saarland University)</i>	
13.00 14.30	Lunch Break				
14.30 16.00	Session 11A Key Exchange Dario Fiore (IMDEA Software Institute)	Session 11B Attacks using a Little Leakage Gang Tan (Penn State University)	Session 11C More Attacks Michael Franz (UC Irvine)	Session 11D Network Security II Tudor Dumitras (UMCP)	Tutorial 7
	A Unilateral-to-Mutual Authentication Compiler for Key Exchange (with Applications to Client Authentication in TLS 1.3) <i>Hugo Krawczyk (IBM Research)</i>	Generic Attacks on Secure Outsourced Databases <i>Georgios Kellaris (Harvard University), George Kollios (Boston University), Kobbi Nissim (Ben-Gurion University) and Adam O'Neill (Georgetown University)</i>	Host of Troubles: Multiple Host Ambiguities in HTTP Implementations <i>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)</i>	Safely Measuring Tor <i>Rob Jansen and Aaron Johnson (U.S. Naval Research Laboratory)</i>	Adversarial Data Mining: Big Data Meets Cyber Security - Part I <i>Murat Kantarcioglu (University of Texas at Dallas, USA) & Bowei Xi (Purdue University, USA)</i>
	Attribute-based Key Exchange with General Policies <i>Vladimir Kolesnikov (Bell Labs), Hugo Krawczyk (IBM Research), Yehuda Lindell (Bar-Ilan University), Alex Malozemoff (Galios) and Tal Rabin (IBM Research)</i>	The Shadow Nemesis: Inference Attacks on Efficiently Deployable, Efficiently Searchable Encryption <i>David Pouliot and Charles V. Wright (Portland State University)</i>	Accessorize to a Crime: Real and Stealthy Attacks on State-Of-The-Art Face Recognition <i>Mahmood Sharif, Sruti Bhagavatula, Lujo Bauer (Carnegie Mellon University) and Michael K. Reiter (University of North Carolina Chapel Hill)</i>	PREDATOR: Proactive Recognition and Elimination of Domain Abuse at Time-Of-Registration <i>Shuang Hao (UC Santa Barbara), Alex Kantchelian (UC Berkeley), Brad Miller (Google), Vern Paxson (UC Berkeley) and Nick Feamster (Princeton University)</i>	
	Identity-Concealed Authenticated Encryption and Key Exchange <i>Yunlei Zhao (Fudan University)</i>	Breaking Web Applications Built On Top of Encrypted Data <i>Paul Grubbs (Cornell University), Richard McPherson (University of Texas, Austin), Muhammed Naveed (University of Southern California), Thomas Risenpart and Vitaly Shmatikov (Cornell Tech)</i>	Lurking Malice in the Cloud: Understanding and Detecting Cloud Repository as a Malicious Service <i>Xiaojing Liao (Georgia Institute of Technology), Sumayah Alrwais, Kan Yuan, Luyi Xing, XiaoFeng Wang (Indiana University Bloomington), Shuang Hao (University of California Santa Barbara) and Raheem Beyah (Georgia Institute of Technology)</i>	Stemming Downlink Leakage from Training Sequences in Multi-User MIMO Networks <i>Yunlong Mao, Yuan Zhang and Sheng Zhong (Nanjing University)</i>	



CCS 2016 Main Conference, Thursday, October 27, 2016

	Track 1 Cryptographic Mechanisms Lecture Hall A	Track 2 Differential Privacy / Cryptography / Attacks Lecture Hall B	Track 3 Web/Mobile Security Lecture Hall C	Track 4 Secure Code and Systems Lecture Hall D	Track 5 Tutorials & Talks Lecture Hall E
16.00 16.30	Coffee Break				
16.30 18.00	Session 12A Secure Protocols Matteo Maffei (Saarland University)	Session 12B DSA/ECDSA Markulf Kohlweiss (Microsoft Research)	Session 12C Even more Attacks Mathias Payer (Purdue University)	Session 12D Censorship Resistance Amir Herzberg (Bar-Ilan University)	Tutorial 7
	A Protocol for Privately Reporting Ad Impressions at Scale <i>Matthew Green (Johns Hopkins University), Watson Ladd (University of California Berkeley) and Ian Miers (Johns Hopkins University)</i>	ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels <i>Daniel Genkin (Technion), Lev Pachmanov, Itamar Pipman, Eran Tromer (Tel Aviv University) and Yuval Yarom (The University of Adelaide)</i>	Android ION Hazard: the Curse of Customizable Memory Management System <i>Hang Zhang, Dongdong She and Zhiyun Qian (University of California, Riverside)</i>	Slitheen: Perfectly imitated decoy routing through traffic replacement <i>Cecylia Bocovich and Ian Goldberg (University of Waterloo)</i>	Adversarial Data Mining: Big Data Meets Cyber Security - Part II <i>Murat Kantarcioglu (University of Texas at Dallas, USA) & Bowei Xi (Purdue University, USA)</i>
	Secure Stable Matching at Scale <i>Jack Doerner, David Evans and Abhi Shelat (University of Virginia)</i>	„Make Sure DSA Signing Exponentiations Really Are Constant-Time“ <i>Cesar Pereida Garcia (Aalto University), Billy Bob Brumley (Tampere University of Technology) and Yuval Yarom (The University of Adelaide)</i>	Coverage-based Greybox Fuzzing as Markov Chain <i>Marcel Boehme, Van-Thuan Pham and Abhik Roychoudhury (National University of Singapore)</i>	Practical Censorship Evasion Leveraging Content Delivery Networks <i>Hadi Zolfaghari and Amir Houmansadr (UMass Amherst)</i>	
	BeleniosRF: A Non-Interactive Receipt-Free Electronic Voting Scheme <i>Pyrros Chaidos, (University College London), Véronique Cortier (CNRS), Georg Fuchsbauer (Inria) and David Galindo (University of Birmingham)</i>	On the Provable Security of (EC)DSA Signatures <i>Manuel Fersch, Eike Kiltz and Bertram Poettering (Ruhr University Bochum)</i>	SFADiff: Automated Evasion Attacks and Fingerprinting Using Blackbox Differential Automata Learning <i>George Argyros (Columbia University), Ioannis Stais (University of Athens), Suman Jana, Angelos Keromytis (Columbia University) and Aggelos Kiayias (University of Edinburgh)</i>	GAME OF DECOYS: Optimal Decoy Routing Through Game Theory <i>Milad Nasr and Amir Houmansadr (UMass Amherst)</i>	
18.05 19.00	CCS Business Meeting Lecture Hall C				
19.00 20.30	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				



Posters

A Behavioural Authentication System for Mobile Users

Md Morshedul 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 Noura (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, Lihua Xu (East China Normal University), Haojin Zhu (Shanghai Jiao Tong University)

An Educational Network Protocol for Covert Channel Analysis Using Patterns

Steffen Wendzel (Fraunhofer FKIE / Worms University of Applied Sciences) and Wojciech Mazurczyk (Warsaw University of Technology)

Attack on Non-Linear Physical Unclonable Function

Jing Ye, Yu 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

Asya Mitseva, Andriy Panchenko (University of Luxembourg), Fabian Lanze (Huf Hülsbeck & Fürst 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 Hohlfeld, Martin Henze, Robin Rawiel, Jan Henrik Ziegeldorf and Klaus Wehrle (RWTH Aachen University)

Identifying Dynamic Data Structures in Malware

Thomas Rupprecht (University of Bamberg), Xi Chen (Vrije Universiteit Amsterdam), David H. White (University of Bamberg), Jan Tobias Mühlberg (KU Leuven), Herbert Bos (Vrije Universiteit Amsterdam) and Gerald Lüttgen (University of Bamberg)

Improved Markov Strength Meters for Passwords

Harshal Tupsamudre, Vijayanand Banahatti and Sachin Lodha (TCS Research)

Insights of Antivirus Relationships when Detecting Android Malware: A Data Analytics Approach

Ignacio Martin, Jose Alberto Hernandez (Universidad Carlos III de Madrid), Sergio de Los Santos and Antonio Guzmán (Telefónica Digital Identity & Privacy)

KXRay: Introspecting the Kernel for Rootkit Timing Footprints

Chen Chen, Darius Suciu and Radu Sion (Stony Brook University)

Locally Virtualized Environment for Mitigating Ransomware Threat

Manish Shukla, Sutapa 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 Asudeh (University of Texas at Arlington) and Matthew Wright (Rochester Institute of Technology)

Privacy Enhanced Secure Location Verification

Md Mamunur Rashid Akand and Rei Safavi-Naini (University of Calgary)

Re-Thinking Risks and Rewards for Trusted Third Parties

Jan-Ole Malchow, Benjamin Gildenring and Volker Roth (Freie Universität Berlin)

RIA: an Audition-based Method to Protect the Runtime Integrity of MapReduce Applications

Yongzhi Wang and Yulong Shen (Xidian University)

Security Enhanced Administrative Role Based Access Control Models

Rajkumar P.V. (Texas Southern University) and Ravi Sandhu (University of Texas at San Antonio)

(Semi)-Supervised Machine Learning Approaches for Network Security in High-Dimensional Network Data

Pedro Casas, Alessandro D'Alconzo, Giuseppe Settanmi (AIT Austrian Institute of Technology), Pierdomenico Fiadino (Eurecat Technology Centre of Catalonia) and Florian Skopik (AIT Austrian Institute of Technology)

Static ROP Chain Detection Based on Hidden Markov Model Considering ROP Chain Integrity

Toshinori Usui (NTT Secure Platform Laboratories), Tomonori Ikuse (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)

Toward Automating the Generation of Malware Analysis Reports Using the Sandbox Logs

Bo Sun, Akinori Fujino and Tatsuya Mori (Waseda University)

Towards Collaboratively Supporting Decision Makers in Choosing Suitable Authentication Schemes

Peter Mayer, Stephan Neumann (Technische Universität Darmstadt) and Melanie Volkamer (Technische Universität Darmstadt & Karlsruher Universität)

Towards Exposing Internet of Things: A Roadmap

Vinay Sachidanand, Jinghui Toh, Shachar Siboni, Asaf Shabtai (Ben-Gurion University of the Negev) and Yuval Elovici (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

Changhee Hahn and Junbeom Hur (Department of Computer Science and Engineering, Korea University)

Vuec – A Framework for Vulnerability Management in Decentralized Communication Networks

Michael Steinke (Universität der Bundeswehr), Stefan Metzger (Leibniz Supercomputing Centre) and Wolfgang Hommel (Universität der Bundeswehr)

Weighing in eHealth Security – A Security and Privacy Study of Smart Scales

Martin Krämer, David Aspinall and Maria Wolters (University of Edinburgh)

WiPING: Wi-Fi signal-based PIN Guessing attack

Seunghun Cha, Jaewoo Park, Geumhwan Cho (Sungkyunkwan University), Jun Ho Huh (Honeywell ACS Labs) and Hyoungshick Kim (Sungkyunkwan University)

Demos

Easy Deployment of a Secure Internet Architecture for the 21st Century - How hard can it be to build a secure Internet?

Ercan Ucan, Raphael M. Reischuk and Adrian Perrig (ETH Zurich)

High-Throughput Secure Three-Party Computation of Kerberos Ticket Generation

Toshinori Araki (NEC Corporation), Assaf Barak (Bar-Ilan University), Jun Furukawa (NEC Corporation), Yehuda Lindell, Ariel Nof (Bar-Ilan University) and Kazuma Ohara (NEC Corporation)

Integrating MPC in Big Data Workflows

Nikolaj Volgushev (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 Johansen and Audun Jøsang (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)

Monday, October 24, Lecture Hall B

PC Chairs: Long Lu (Stony Brook University, USA), Mohammad Mannan (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 Ekberg (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.** Shinjo Park, Altaf Shaik (TU Berlin/Telekom Innovation Labs), Ravishankar Borgaonkar (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, Yueqian Zhang (Tsinghua University), Zhou Li (ACM Member) and Haixin Duan (Tsinghua University)**CRiOS: Toward Large-Scale iOS Application Analysis.** Damilola Orikogbo, 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)**On a (Per)Mission: Building Privacy Into the App Marketplace.** Hannah Quay-De La Vallee, Paige Selby and Shriram Krishnamurthi (Brown University)**Exploiting Phone Numbers and Cross-Application Features in Targeted Mobile Attacks.** Srishri Gupta (Indraprastha Institute of Information Technology, Delhi), Payas Gupta (School of Information Systems, Singapore Management University), Mustaque Ahmad (Georgia Institute of Technology & New York University Abu Dhabi) and Ponnurangam Kumaraguru (IIITD)

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 (Telefonica), Kari Kostianen and Srdjan Capkun (ETH Zurich)**Picasso: Lightweight Device Class Fingerprinting for Web Clients.** Elie Bursztein, Artem Malyshev, Tadek Pietraszek and Kurt Thomas (Google)**Detecting Misuse of Google Cloud Messaging in Android Badware.** Mansour Ahmadi, Battista Biggio (University of Cagliari), Steven Arzt (Technische Universität Darmstadt), Davide Ariu and Giorgio Giacinto (University of Cagliari)**On the CCA (in)security of MTPProto. (short paper)** Jakob Jakobsen and Claudio Orlandi (Aarhus University)**Breaking TETRA Location Privacy and Network Availability. (short paper)** Martin Pfeiffer, Jan-Pascal Kwiotek, Jiska Classen, Robin Klose and Matthias Hollick (Secure Mobile Networking Lab, TU Darmstadt)

Workshop on Privacy in the Electronic Society (WPES 2016)

Monday, October 24, Lecture Hall E

PC Chair: Sabrina De Capitani di Vimercati (Università degli Studi di Milano, Italy)

07.30 – 08.25 Registration & Early Bird Coffee

08.25 – 10.30 Welcome & Session 1: User Privacy

Session Chair: Yazan Boshmaf (Qatar Computing Research Institute, Qatar)

An Efficient and Robust Social Network De-anonymization Attack Gabor Gyorgy Gulyas (INRIA), Benedek Simon and Sándor Imre (BME)**Control Versus Effort in Privacy Warnings for Webforms** Kat Krol (Univ. College London) and Sören Preibusch (Microsoft Research)**On Profile Linkability despite Anonymity in Social Media Systems** Michael Backes, Pascal Berrang (CISPA, Saarland Univ.), Oana Goga (MPI-SWS), Krishna Gummad (MPI-SWS) and Praveen Manoharan (CISPA, Saarland Univ.)**Disguised Chromium Browser: Robust browser, Flash and Canvas Fingerprinting Protection** Martin Stopczynski, Peter Baumann, Stefan Katzenbeisser (TUD) and Erik Tews (Univ. of Birmingham)**Predicting Mobile App Privacy Preferences with Psychographics** Andrew McNamara, Akash Verma, Jon Stallings and Jessica Staddon (N.C. State Univ.)

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 Sluganovic, Ivan Martinovic (Univ. of Oxford), Gene Tsudik (Univ. of California) and Kasper Bonne Rasmussen (Univ. of Oxford)**That's the Way the Cookie Crumbles: Evaluating HTTPS Enforcing Mechanisms** Suphannee Sivakorn, Angelos Keromytis (Columbia Univ.) and Jason Polakis (Univ. of Illinois at Chicago)**Detecting Communities under Differential Privacy** Huu-Hiep Nguyen, Abdessamad Imine and Michael Rusinowitch (LORIA/INRIA Nancy)**Poisoning the Well - Exploring the Great Firewall's Poisoned DNS Responses** Oliver Farnan (Univ. of Oxford), Alex Darer (Oxford Internet Institute) and Joss Wright (Univ. of Oxford)

12.30 – 13.45 Lunch

13.45 – 15.30 Session 3: Privacy Policies and Anonymous Credentials

Session Chair: Adam J. Lee (University of Pittsburgh)

CPPL: Compact Privacy Policy Language Martin Henze, Jens Hiller, Sascha Schmerling, Jan Henrik Ziegeldorf and Klaus Wehrle (RWTH Aachen Univ.)**Vote to Link: Recovering from Misbehaving Anonymous Users** Wouter Lueks (Radboud Univ.), Maarten Everts (TNO Netherlands) and Jaap-Henk Hoepman (Radboud Univ.)**Scalable Revocation Scheme for Anonymous Credentials Based on n-times Unlinkable Proofs** Jan Camenisch, Manu Drijvers (IBM Research) and Jan Hajny (Brno Univ. of Technology)**Automatic Assessment of Website Compliance to the European Cookie Law with CoolCheck** Claudio Carpineto (Fondazione Ugo Bordoni), Davide Lo Re (Univ. of Rome 1) and Giovanni Romano (Fondazione Ugo Bordoni)**UnlimitID: Privacy-Preserving Federated Identity Management using Algebraic MACs** Marios Isaakidis (Univ. College London), Harry Halpin (INRIA) and George Danezis (Univ. College London)

15.30 – 16.00 Coffee Break

16.00 – 18.10 Session 4: Data privacy and Anonymous Communication

Session Chair: Panos Papadimitratos (KTH, Sweden)

(The Futility of) Data Privacy in Content-Centric Networking Christopher A. Wood, Cesar Ghalí and Gene Tsudik (Univ. of California Irvine)**Elxa: Scalable Privacy-Preserving Plagiarism Detection** Nik Unger, Sahithi Thandra and Ian Goldberg (Univ. of Waterloo)**ABRA CADABRA: Magically Increasing Network Utilization in Tor by Avoiding Bottlenecks** John Geddes, Michael Schliep and Nicholas Hopper (Univ. of Minnesota)**TASP: Towards Anonymity Sets that Persist** Jamie Hayes (Univ. College London), Carmela Troncoso (IMDEA Software Institute) and George Danezis (Univ. College London)**PriFi: A Low-Latency and Tracking-Resistant Protocol for Local-Area Anonymous Communication** Ludovic Barman (EPFL), Mahdi Zamani (Yale Univ.), Italo Dacosta (EPFL, Switzerland), Joan Feigenbaum (Yale Univ.), Bryan Ford, Jean-Pierre Hubaux (EPFL) and David Wolinsky (Facebook)**Privacy-Preserving Lawful Contact Chaining** Aaron Segal, Joan Feigenbaum (Yale Univ.) and Bryan Ford (EPFL)

Monday, October 24, 2016

3rd ACM Workshop on Information Sharing and Collaborative Security (WISCS 2016)

Monday, October 24, Lecture Hall F

PC Chairs: Florian Kerschbaum (SAP), Erik-Oliver Blass (Airbus Group Innovations)

07.30 – 09.00 Registration & Early-Bird Coffee**09.00 – 10.30 Welcome and Session 1: Keynote**
Session Chair: Florian Kerschbaum (SAP)**Keynote: Back to the Roots: Information Sharing Economics and What We Can Learn for Security.** Rainer Böhme (University of Innsbruck)**10.30 – 11.00 Coffee Break****11.00 – 12.30 Session 2: Models for Information Sharing Intelligence**

Session Chair: Rainer Böhme (University of Innsbruck)

A Model for Secure and Mutually Beneficial Software Vulnerability Sharing. Alex Davidson, Gregory Fenn and Carlos Cid (Royal Holloway University of London)**Shall we collaborate? A model to analyse the benefits of information sharing.** Roberto Garrido, Lorena Gonzalez and Sergio Pastrana (Carlos III University of Madrid)**Collaborative Incident Handling Based on the Blackboard-Pattern.** Nadine Herold, Holger Kinkel and Georg Carle (Technical University of Munich)**12.30 – 14.00 Lunch****14.00 - 15.00 Session 3: Tools for Information Sharing**

Session Chair: Jose Such (Lancaster University)

Private Sharing of IOCs and Sightings (short paper). Tim R. van de Kamp, Andreas Peter, Maarten H. Everts and Willem Jonker (University of Twente)**Managing Data Sharing in OpenStack Swift with Over-Encryption.** Enrico Bacis (Università degli Studi di Bergamo), Sabrina De Capitani di Vimercati, Sara Foresti (Università degli Studi di Milano), Daniele Guttadoro, Stefano Paraboschi, Marco Rosa (Università degli Studi di Bergamo), Pierangela Samarati (Università degli Studi di Milano) and Alessandro Saullo (Università degli Studi di Bergamo)**MISP - The design and implementation of a collaborative threat intelligence sharing platform.** Cynthia Wagner (RESTENA Foundation), Alexandre Dulaunoy, Gérard Wagener and Andras Iklody (CIRCL)**15.30 – 16.00 Coffee Break****16.00 – 17.30 Session 4: Real-World Studies**
Session Chair: Erik-Oliver Blass (Airbus Group Innovations)**Privacy Risk in Cybersecurity Data Sharing.** Jaspreet Bhatia, Travis Breaux (CMU), Liora Friedberg (UPenn), Hanan Hibshi and Daniel Smullen (CMU)**Data quality challenges and future research directions in threat intelligence sharing practice.** Christian Sillaber, Clemens Sauerwein and Ruth Breu (University of Innsbruck)**Measuring the Impact of Sharing Abuse Data with Web Hosting Providers.** Marie Vasek, Matthew Weeden and Tyler Moore (University of Tulsa)**Third ACM Workshop on Moving Target Defense (MTD 2016)**

Monday, October 24, Lecture Hall G

PC Chairs: Peng Liu (Penn State University, USA), Cliff Wang (U.S. Army Research Office, USA)

07.30 – 08.50 Registration & Early Bird Coffee**08.50 – 10.00 Welcome and Keynote**
Session Chair: Peng Liu (Penn State University)**Keynote: A Cyber Mutation: Metrics, Techniques and Future Directions.** Ehab Al-Shaer (University of North Carolina, Charlotte)**10.00 – 11.00 Session 1: New Moving Target Defenses (I)****Have No PHEAR: Networks Without Identifiers.** Richard Skowrya, Kevin Bauer, Veer Dedhia and Hamed Okhravi (MIT Lincoln Laboratory)**Towards Cost-Effective Moving Target Defense Against DDoS and Covert Channel Attacks.** Huangxin Wang, Fei Li and Songqing Chen (GMU)**11.00 – 11.20 Coffee Break****11.20 – 12.50 Session 2: New Moving Target Defenses (II)****SDN based scalable MTD solution in Cloud. Network** Ankur Chowdhary, Sandeep Pisharody and Dijiang Huang (ASU)**A Moving Target Defense Approach to Disrupting Stealthy Botnets.** Sridhar Venkatesan, Massimiliano Albanese (GMU), George Cybenko (Dartmouth College) and Sushil Jajodia (GMU)**Multi-dimensional Host Identity Anonymization for Defeating Skilled Attackers.** Jafar Haadi Jafarian, Amirreza Niakanlahiji, Ehab Al-Shaer and Qi Duan (UNCC)**12.50 – 14.00 Lunch Break & System Demo****13.40 – 14.20 System Demo****Demo: A Symbolic N-Variant System** Jun Xu, Pinyao Guo (PSU), Bo Chen (Memphis University), Robert F. Erbacher (ARL), Ping Chen and Peng Liu (PSU)**14.20 – 14.50 Industry Talk**

Session Chair: Peng Liu (Penn State University)

Industry Talk: Moving Target Defense - A Journey from Idea to Product. Jason Li (Intelligent Automation, Inc.)**14.50 – 15.50 Session 3: Modeling and Evaluation of Moving Target Defenses (I)**

Session Chair: Hamed Okhravi (MIT Lincoln Laboratory)

Markov Modeling of Moving Target Defense.**Games** Saeed Valizadeh, Hoda Maleki (UConn), William Koch, Azer Bestavros (Boston Univ.) and Marten van Dijk (UConn)**Moving Target Defense against DDoS Attacks: An Empirical Game-Theoretic Analysis.** Mason Wright (University of Michigan), Sridhar Venkatesan (GMU), Massimiliano Albanese (GMU) and Michael Wellman (University of Michigan)**15.50 – 16.05 Coffee Break****16.05 – 17.35 Session 4: Modeling and Evaluation of Moving Target Defenses (II)****Graph Analysis and Moving Target Defense Selection.** Christopher Lamb and Jason Hamlet (Sandia National Laboratories)**Formal Approach for Resilient Reachability based on End-System Route Agility.** Usman Rauf, Fida Gillani, Ehab Al-Shaer (UNCC), Mahantesh Halappanavar, Samrat Chatterjee and Christopher Oehmen (PNNL)**Mayflies: A Moving Target Defense Framework for Distributed Systems. (short paper)** Noor Ahmed (AFRL) and Bharat Bhargava (Purdue University)**Automated Effectiveness Evaluation of Moving Target Defenses: Metrics for Missions and Attacks. (short paper)** Joshua Taylor, Kara Zaffarano, Ben Koller, Charlie Bancroft and Jason Syversen (Siege Technologies)**17.35 – 17.40 Wrap up**

Monday, October 24, 2016



Testing and Evaluation for Active & Resilient Cyber Systems (SafeConfig 2016) Monday, October 24, Lecture Hall H <i>PC Chairs: David Manz (Pacific Northwest National Laboratory, USA), Anoop Singhal (National Institute of Standards and Technology, USA), Nick Multari (Pacific Northwest National Laboratory, USA)</i>	
07.30 – 09.00 Registration & Early Bird Coffee	14.00 – 15.30 Session 2 <i>Session Chair: David Manz (Pacific Northwest National Laboratory)</i>
09.00 – 10.35 Welcome and Keynotes	Firewalling Scenic Routes: Preventing Data Exfiltration via Political and Geographic Routing Policies. <i>Kevin Benton and L. Jean Camp (Indiana Univ)</i>
Keynote: Configuring Software and Systems for Defense-in-Depth. <i>Trent Jaeger (Penn State Univ)</i>	An Iterative and Toolchain-Based Approach to Automate Scanning and Mapping Computer Networks. <i>Stefan Marksteiner, Harald Lernbeiss and Bernhard Jandl-Scherf (Joanneum Research)</i>
Keynote: From cyber security to collaborative cyber resiliency. <i>George Sharkov (Government of Bulgaria)</i>	A Graph-Based Impact Metric for Mitigating Lateral Movement Cyber Attacks. <i>Emilie Purvine, John R. Johnson and Chaomei Lo (PNNL)</i>
10.35 – 11.00 Coffee Break	15.30 -16.00 Coffee Break
11.00 – 12.30 Session 1 <i>Session Chair: Nick Multari (Pacific Northwest National Laboratory)</i>	16.00 – 17.30 Panel Discussion: Testing and Evaluation for Active and Resilient Cyber Systems <i>Session Chair: David Manz (Pacific Northwest National Laboratory)</i>
AHEAD: A New Architecture for Active Defense. <i>Fabio De Gaspari (Sapienza Univ), Sushil Jajodia (George Mason Univ), Luigi V. Mancini and Agostino Panico (Sapienza Univ)</i>	Panelists: <ul style="list-style-type: none">• 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)
A One-Year Perspective on Exposed In-memory Key-Value Stores. <i>Tobias Fiebig, Anja Feldmann and Matthias Petschick (TU Berlin)</i>	
Towards Automated Verification of Active Cyber Defense Strategies on Software Defined Network. <i>Mohammed Alsaleh and Ehab Al-Shaer (UNCC)</i>	
12.30 – 14.00 Lunch Break	

Theory of Implementation Security (TIS 2016) Monday, October 24, Lecture Hall I <i>PC Chairs: Begül Bilgin, Svetla Nikova, Vincent Rijmen (KU Leuven, Belgium)</i>	
07.30 – 09.00 Registration & Early-Bird Coffee	12.30 – 14.00 Lunch Break
09.00 – 10.30 Welcome and Session 1 <i>Session Chair: Vincent Rijmen (KU Leuven, Belgium)</i>	14.00 – 15.30 Session 3 <i>Session Chair: Svetla Nikova (KU Leuven, Belgium)</i>
Invited Talk: Masking and MPC: When Crypto Theory Meets Crypto Practice. <i>Nigel Smart (University of Bristol)</i>	Invited Talk: On Non-uniformity in Threshold Sharings. <i>Joan Daemen (Radboud University Nijmegen and STMicroelectronics)</i>
Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order. <i>Hannes Gross, Stefan Mangard, Thomas Korak (IAIK, Graz University of Technology)</i>	ParTI - Towards Combined Hardware Countermeasures against Side-Channel and Fault-Injection Attacks. <i>Tobias Schneider, Amir Moradi, Tim Güneysu (Ruhr Universität Bochum)</i>
10.30 – 11.00 Coffee Break	15.30 – 16.00 Coffee Break
11.00 – 12.30 Session 2 <i>Session Chair: Begül Bilgin (KU Leuven, Belgium)</i>	16.00 – 17.30 Session 4 <i>Session Chair: Svetla Nikova (KU Leuven, Belgium)</i>
Moments-Correlating DPA. <i>Amir Moradi (Ruhr Universität Bochum), François-Xavier Standaert (Université catholique de Louvain)</i>	Invited Talk: Threshold Implementations in Industry: A Case Study on SHA-25. <i>Mike Hutter (Cryptography Research – Rambus)</i>
Hiding Higher-Order Univariate Leakages by Shuffling Polynomial Masking Schemes. <i>Fabrizio De Santis, Tobias Bauer and Georg Sigl (Technische Universität München)</i>	Masking AES with d+1 Shares in Hardware. <i>Thomas De Cnudde, Oscar Reparaz, Begül Bilgin, Svetla Nikova, Ventzislav Nikov, Vincent Rijmen (KU Leuven, NXP)</i>
Practical Results of ECC Side Channel Countermeasures on an ARM Cortex M3 Processor. <i>Jacek Samotyjka and Kerstin Lemke-Rust (Bonn-Rhein-Sieg University of Applied Sciences)</i>	

ACM SIGPLAN 11th Workshop on Programming Languages and Analysis for Security (PLAS 2016)

Monday, October 24, Lecture Hall J

PC Chairs: Toby Murray (University of Melbourne and Data61), Deian Stefan (UC San Diego and Intrinsic)

07.30 – 08.50 Registration & Early-Bird Coffee

08.50 – 10.30 Welcome and Session 1: JavaScript

Session Chair: Deian Stefan (UC San Diego and Intrinsic)

Invited Talk: Flow: Analysis of JavaScript for type checking and beyond. Avik Chaudhuri (Facebook)**Static Detection of User-specified Security Vulnerabilities in Client-side JavaScript.** Jens Nicolay, Valentijn Spruyt and Coen De Roover (Vrije Universiteit Brussel)

10.30 – 11.00 Coffee Break

11.00 – 12.30 Session 2: Information Flow
Session Chair: Tamara Rezk (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.** Sepehr Amir-Mohammadian and Christian Skalk (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 Bielova (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.** Cédric Fournet (Microsoft Research)**Formal Verification of Smart Contracts. (short paper)** Karthikeyan Bhargavan (INRIA), Antoine Delignat-Lavaud, Cédric Fournet (Microsoft Research), Anitha Gollamudi (Harvard University), Georges Gonthier (Microsoft Research), Nadim Kobeissi (INRIA), Aseem Rastogi (Harvard University), Thomas Sibut-Pinote (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)

8th ACM Cloud Computing Security Workshop (CCSW 2016)

Friday, October 28, Lecture Hall B

PC Chairs: Elli Androulaki (IBM Research – Zurich), Mike Reiter (University of North Carolina at Chapel Hill)

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 Franceschina (Teralytics)**Co-Location Resistant Strategy with Full Resources Optimization.** Berrima Mouheb (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 Abdelraheem, Christian Gehrman, Lindström and Christian Nordahl (Swedish Institute of Computer Science)**Poly-Logarithmic Range Queries on Encrypted Data with Small Leakage.** Florian Hahn and Florian Kerschbaum (SAP)**Encrypting Analytical Web Applications.** Benny Fuhry, 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.** Meryeme Ayache, Mohamed Erradi (ENSLAS, Mohammed V University), Ahmed Khoumsi and (University of Sherbrooke)

15.30 - 16.00 Coffee Break

16.00 - 18.00 Session 4: Secure storage and storage efficiency

On Information Leakage in Deduplicated Storage Systems. Hubert Ritzdorf (ETH Zurich, Switzerland), Ghassan Karame (NEC Laboratories Europe, Germany), Claudio Soriente (Telefonica, Spain) and Srdjan Capkun (ETH Zurich, Switzerland)**Message-Locked Proofs of Retrievability with Secure Deduplication.** Dimitrios Vasilopoulos, Melek Önen, Kaoutar Elkhiyaoui and Refik Molva (EURECOM)**Generic Efficient Dynamic Proofs of Retrievability.** Mohammad Etemad and Alptekin Küpçü (Koç University)**Assured Deletion in the Cloud: Requirements, Challenges and Future Directions.** Kopo M. Ramokupane, Awais Rashid and Jose M. Such (Lancaster University)

18.00 – 18.10 Closing

Monday, October 24, 2016

Friday, October 28, 2016



Second ACM Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC 2016) Friday, October 28, Lecture Hall E <i>PC Chairs: Rakesh Bobba (Oregon State University, USA), Alvaro Cardenas (University of Texas at Dallas, USA)</i>	
07.30 - 08.50 Registration & Early Bird Coffee	14.00 - 15.30 Session 3: Risk Assessment and Resilience <i>Session Chair: Nils Ole Tippenhauer (Singapore University of Technology and Design)</i>
8.50 - 10.30 Welcome and Session 1: Industrial Control Systems <i>Session Chair: Michail Maniatakos (New York University, Abu Dhabi)</i>	Evaluating Resilience of Gas Pipeline Systems Under Cyber-Physical Attacks: A Function-Based Methodology. <i>Yatin Wadhawan (University of Southern California) and Clifford Neuman (Information Science Institute, USC)</i>
Automatic Construction of Statechart-Based Anomaly Detection Models for Multi-Threaded SCADA via Spectral Analysis. <i>Amit Kleinmann and Avishai Wool (Tel-Aviv University)</i>	A Case Study on Implementing False Data Injection Attacks Against Nonlinear State Estimation. <i>Charalambos Konstantinou (New York University) and Michail Maniatakos (New York University, Abu Dhabi)</i>
Towards High-Interaction Virtual ICS Honeypots-in-a-Box. <i>Daniele Antonioli, Anand Agrawal and Nils Ole Tippenhauer (Singapore University of Technology and Design)</i>	Achieving ICS Resilience and Security through Granular Data Flow Management. <i>Benjamin Green (Lancaster University), Marina Krotofil (Honeywell Cyber Security Lab) and David Hutchison (Lancaster University)</i>
SENAMI: Selective Non-Invasive Active Monitoring for ICS Intrusion Detection. <i>William Jardine, Sylvain Frey, Benjamin Green and Awais Rashid (Lancaster University)</i>	15.30 - 16.00 Coffee Break
10.30 - 11.00 Coffee Break	16.00 - 17.30 Session 4: Insights from Testbeds and Games <i>Session Chair: Awais Rashid (Lancaster University, UK)</i>
11.00 - 12.30 Session 2: Vehicular CPS <i>Session Chair: Pauline Anthonysamy (Google, Switzerland)</i>	HAMIDS: An Hierarchical Monitoring Intrusion Detection System for Industrial Control Systems. <i>Hamid Reza Ghaeini and Nils Ole Tippenhauer (Singapore University of Technology and Design)</i>
Secure Location Verification with a Mobile Receiver. <i>Richard Baker and Ivan Martinovic (University of Oxford)</i>	SoftGrid: A Software-based Smart Grid Testbed for Evaluating Substation Cybersecurity Solutions. <i>Prageeth Gunathilaka, Daisuke Mashima and Binbin Chen (Advanced Digital Sciences Center, Singapore)</i>
Risk Assessment for Cooperative Automated Driving. <i>Derrick Dominic (University of Michigan), Sumeet Chhawri (UMTRI), Ryan Eustice (University of Michigan), Di Ma (University of Michigan-Dearborn) and Andre Weimerskirch (University of Michigan)</i>	Exposing Transmitters in Mobile Multi-Agent Games. <i>Mai Ben Adar - Bessos (Bar - Ilan University), Simon Birnbach (University of Oxford), Amir Herzberg (Bar-Ilan University) and Ivan Martinovic (University of Oxford)</i>
Towards Safe and Secure Autonomous and Cooperative Vehicle Ecosystems. <i>Antonio Lima, Francisco Rocha, Marcus Völp and Paulo Esteves-Verissimo (University of Luxembourg)</i>	
12.30 - 14.00 Lunch Break	

6th International Workshop on Trustworthy Embedded Devices (TrustedED 2016) Friday, October 28, Lecture Hall F <i>PC Chairs: Xinxin Fan (Robert Bosch LLC, US), Tim Güneysu (University of Bremen & DFKI, DE)</i>	
07.30 - 09.00 Registration & Early Bird Coffee	12.30 - 14.00 Lunch Break
09.00 - 10.30 Session 1: Trusted Device Internals <i>Session Chair: Tim Güneysu (University of Bremen & DFKI, DE)</i>	14.00 - 15.30 Session 3: Attacks on Secured Channels <i>Session Chair: Markus Dürmuth (Ruhr-Universität Bochum, DE)</i>
Keynote: Analyzing Thousands of Firmware Images and a Few Physical Devices. What's Next? <i>Aurelien Francillon (EURECOM, FR)</i>	Keynote: Wireless Attacks on Automotive Remote Keyless Entry Systems. <i>David Oswald (University of Birmingham, UK)</i>
Side-channel attacks on fingerprint matching algorithms. <i>Markus Dürmuth (Ruhr-Universität Bochum, DE), David Oswald (University of Birmingham, UK) and Niklas Pastewka (Ruhr-Universität Bochum, DE)</i>	Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations. <i>Andrei Costin (EURECOM, FR)</i>
10.30 - 11.00 Coffee Break	15.30 - 16.00 Coffee Break
11.00 - 12.30 Session 2: Trusted Physical Entities <i>Session Chair: Marcel Medwed (NXP, AT)</i>	16.00 - 17.30 Session 4: IoT Security <i>Session Chair: Xinxin Fan (Robert Bosch LLC, US)</i>
Online Reliability Testing for PUF Key Derivation. <i>Matthias Hiller, Aysun Gurur Önalán, Georg Sigl (Technical University of Munich, DE) and Martin Bossert (University of Ulm, DE)</i>	Keynote: IoT Security Challenges and Ways Forward. <i>Marcel Medwed (NXP, AT)</i>
Evaluation of Latch-based Physical Random Number Generator Implementation on 40nm ASICs. <i>Naoya Torii, Dai Yamamoto (FUJITSU Laboratories Ltd, JP) and Tsutomu Matsumoto (Yokohama National University, JP)</i>	Looks Good To Me: Authentication for Augmented Reality. <i>Ethan Gaebel, Ning Zhang, Wenjing Lou and Y. Thomas Hou (VirginiaTech, US)</i>
On the Energy Cost of Channel Based Key Agreement. <i>Christopher Huth, Rene Guillaume, Paul Duplys, Kumaragurubaran Velmurugan (Robert Bosch GmbH, DE) and Tim Güneysu (University of Bremen & DFKI, DE)</i>	

The 2016 Workshop on Forming an Ecosystem Around Software Transformation (FEAST 2016)

Friday, October 28, Lecture Hall G

PC Chairs: Sukarno Mertoguno, Ryan Craven and Gary Toth (Office of Naval Research, USA)

07.30 - 08.30 Registration & Early Bird Coffee

08.30 – 10.30 Welcome and Session 1: dLB: Software transformation methods and challenges
Session Chair: Don Wagner (Office of Naval Research)

Software Transformation: Applications, Tools, Challenges, and Program Representation. *Eric Schulte, Michael McDougall and Dave Melski (Grammtech)*

Beyond Binary Program Transformation. *Bruno Dutertre, Ashish Gehani, Hassen Saidi, Martin Schäff and Ashish Tiwari (SRI International)*

XS-Shredder: A Cross-Layer Framework for Removing Code Bloat in Web Applications. *Adam Doupe (ASU), Alexandros Kapravelos (NCSU), Manuel Egele (BU) and Nick Nikiforakis (Stony Brook)*

A New Direction for Reverse Engineering. *Dinghao Wu (Penn State)*

Open discussion led by session chair.

10.30 – 11.00 Coffee Break

11.00 – 12.30 Session 2: FIR: Application feature identification and removal, including approaches for feature-code association
Session Chair: Ryan Craven (Office of Naval Research)

Feature Identification and Removal for Legacy Binaries. *Xiangyu Zhang and Dongyan Xu (Purdue)*

Binary Software Complexity Reduction: From Artifact to Feature Removal. *Masoud Ghaffarinia and Kevin Hamlen (UT Dallas)*

Software Customization and Bloatware Mitigation Based on Static Analysis. *Dinghao Wu*

Open discussion led by session chair.

12.30 – 14.00 Lunch

14.00 – 15.30 Session 3: V&V: Verification and model extraction of transformed software
Session Chair: Sukarno Mertoguno (Office of Naval Research)

Applications of Binary Analysis and Transformation in Security and Optimization. *Joe Hendrix, Tristan Ravitch and Simon Winwood (Galois)*

Safety-Security Control Code Verification. *Saman Zonouz (Rutgers)*

A Bottom-Up Verification Approach for Systems Software. *Yakoub 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; foundations and enablers for software transformation
Session Chair: Gary Toth (Office of Naval Research)

De-Inductive Reasoning and Explanation for Cybersecurity Threats (DIRECT). *Anupam Datta (CMU), Matt Fredrikson (CMU), Joel Hypolite (UPenn), Andrew Myers (Cornell), Jonathan Smith (UPenn), Andre Scedrov (UPenn), Carolyn Talcott (SRI) and Nathan Dautenhahn (UPenn)*

libdetox: A Framework for Online Program Transformation. *Mathias Payer (Purdue)*

ALLVM. *Will Dietz and Vikram Adve (UIUC)*

Runtime Transformation through Augmented Binary Analysis. *David Williams-King and Junfeng Yang (Columbia)*

Open discussion led by session chair.

Closing Remarks. *Gary Toth and Ryan Craven (ONR)*

8th ACM CCS International Workshop on Managing Insider Security Threats (MIST 2016)

Friday, October 28, Lecture Hall H

PC Chairs: Ilun You (Soonchunhyang University, Republic of Korea), Elisa Bertino (Purdue University USA)

07.30 - 08.50 Registration & Early Bird Coffee

08.50 - 10.30 Welcome and Session 1: Access Control & Application Security
Session Chair: Ioannis Agraftiotis (Oxford University, UK)

A Grey-Box Approach for Detecting Malicious User Interactions in Web Applications. *Wafa Ben Jaballah and Nizar Kheir (Orange Labs, France)*

Restricting Insider Access through Efficient Implementation of Multi-Policy Access Control Systems. *Peter Mell, James Shook and Serban Gavrila (National Institute of Standards and Technology, USA)*

Towards Formal Analysis of Insider Threats for Auctions. *Florian Kammueeller (Middlesex University London, UK and TU Berlin, Germany), Manfred Kerber (University of Birmingham, UK) and Christian W. Probst (Technical University of Denmark, Denmark)*

10.30 - 11.00 Coffee Break

11.00 - 12.30 Session 2 – Best Paper
Session Chair: Christian W. Probst (Technical University of Denmark, Denmark)

Studying Naive Users and the Insider Threat with SimpleFlow. *Ryan Johnson, Jessie Lass and W. Michael Petullo (United States Military Academy, USA)*

A New Take on Detecting Insider Threats: Exploring the use of Hidden Markov Models. *Tabish Rashid, Ioannis Agraftiotis and Jason R.C. Nurse (Oxford University, UK)*

12.30 - 14.00 Lunch Break

14.00 - 15.30 Session 3 - Cyber Attacks & Network Security

Session Chair: Florian Kammueeller (Middlesex University London and TU Berlin)

Cyber Deception: Virtual Networks to Defend Insider Reconnaissance. *Stefan Achleitner, Thomas La Porta, Patrick McDaniel (Pennsylvania State University, USA), Shridatt Sugrim (Applied Communication Sciences, USA), Srikanth Krishnamurthy (University of California, Riverside, USA) and Ritu Chadha (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 Jiaotong University, China), Ziwei Hu (Global Energy Interconnection Research Institute, China) and Ilun You (Soonchunhyang University, Republic of Korea)*

15.30 - 16.00 Coffee Break

16.00 - 17.30 Session 4 – short paper
Session Chair: Ilun You (Soonchunhyang University, Republic of Korea)

Function-Based Access Control (FBAC): From Access Control Matrix to Access Control Tensor. *Yvo Desmedt (The University of Texas at Dallas and University College London, USA) and Arash Shaghaghi (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 Naghmouchi, Nancy Perrot (Orange Labs, France), Ridha Mahjoub (LAMSAD, University Paris-Dauphine), Nizar Kheir and Jean-Philippe Wary (Orange Labs, France)*

Online and offline security policy assessment. *Fulvio Valenza, Marco Vallini and Antonio Lioy (Politecnico di Torino, Italy)*

A tripwire grammar for insider-threat detection. *Ioannis Agraftiotis, Arnau Erola, Michael Goldsmith and Sadie Creese (Oxford University, UK)*

Discovering Insider Threats from Log Data with High-Performance Bioinformatics Tools. *Markus Wurzenberger, Florian Skopik, 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, Hyeungjun Yeuk, Kangbin Yim (Soonchunhyang University, Republic of Korea) and Suhyun Kim (IoT Security Research Center, Soonchunhyang University, Republic of Korea)*

Friday, October 28, 2016

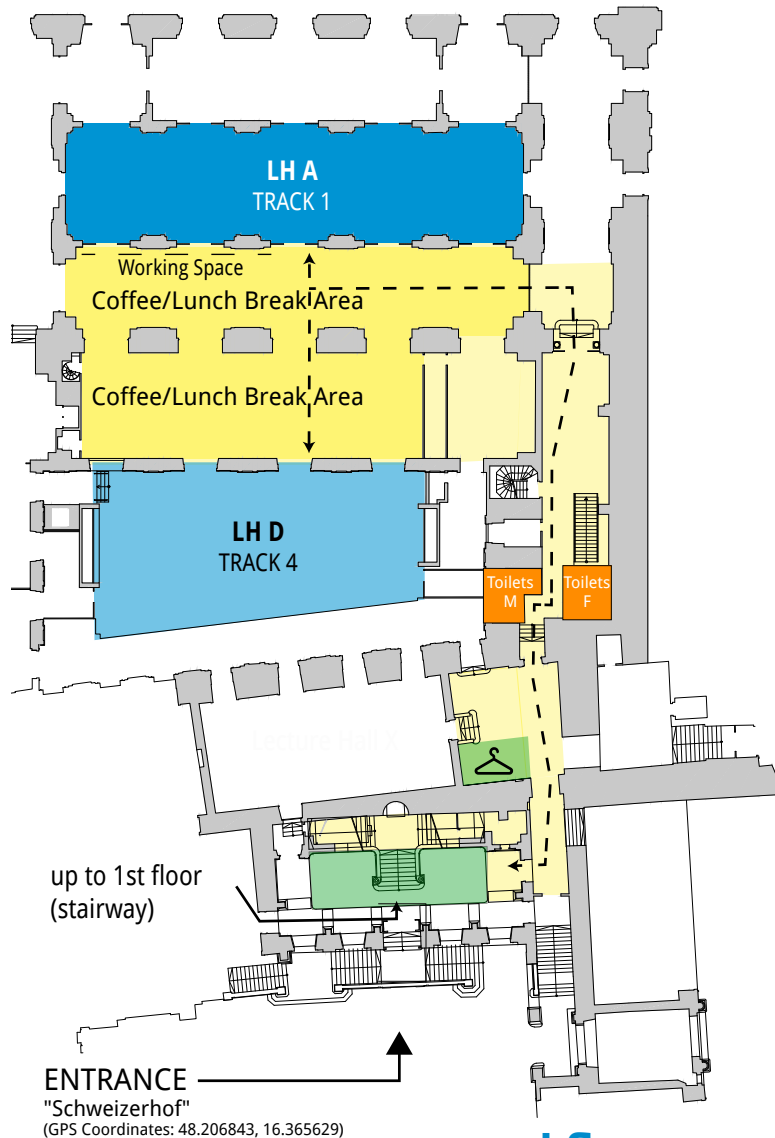


2nd International Workshop on Software PROtection (SPRO 2016) Friday, October 28, Lecture Hall I <i>Chairs: Bjorn De Sutter (Ghent University, Belgium), Brecht Wyseur (NAGRA, Switzerland)</i>	
07.30 – 08.30 Registration & Early Bird Coffee	12.30 – 14.00 Lunch Break
08.30 – 09.30 Welcome and Session 1: Keynote Keynote: Intel Software Guard Extensions – Introduction and Open Research Challenges. <i>Matthias Schunter (Intel Collaborative Research Institute for Secure Computing and Intel Labs)</i>	14.00 – 15.30 Session 4: White-box Crypto & Integrity <i>Session Chair: Christian Mönch (Conax)</i> StlIns4CS: A State Inspection Tool for C#. <i>Amjad Ibrahim and Sebastian Banescu (Technische Universität München)</i>
09.30 – 10.30 Session 2: Vulnerabilities <i>Session Chair: Jack Davidson (University of Virginia)</i> Beyond the Attack Surface: Assessing Security Risk with Random Walks on Call Graphs. <i>Nathan Munaiah and Andrew Meneely (Rochester Institute of Technology)</i>	Reactive Attestation: Automatic Detection and Reaction to Software Tampering Attacks. <i>Alessio Viticchié (Politecnico di Torino), Andrea Avancini, Mariano Ceccato (Fondazione Bruno Kessler), Cataldo Basile (Politecnico di Torino), Bert Abrath and Bart Coppens (Ghent University)</i>
ROP Gadget Prevalence and Survival under Compiler-based Binary Diversification Schemes. <i>Joel Coffman, Daniel Kelly, Christopher Wellons and Andrew Gearhart (Johns Hopkins University Applied Physics Laboratory)</i>	Attacking White-Box AES Constructions. <i>Brendan McMillan and Nick Sullivan (CloudFlare)</i>
10.30 – 11.00 Coffee Break	15.30 – 16.00 Coffee Break
11.00 – 12.30 Session 3: Obfuscation <i>Session Chair: Johannes Kinder (Royal Holloway, University of London)</i>	16.00 – 16.30 Session 5: Panel Discussion <i>Session Chair: Brecht Wyseur (NAGRA, Switzerland)</i> Software Protection Research in Europe, where are we going?
Defeating MBA-based Obfuscation. <i>Ninon Eyrolles (Quarkslab), Louis Goubin (UVSQ, Laboratoire de mathématiques) and Marion Videau (Quarkslab and LORIA)</i>	16.30 – 18.00 Session 6: Hands-on Tutorial The ASPIRE Framework for Software Protection. <i>ASPIRE consortium</i>
VOT4CS: A Virtualization Obfuscation Tool for C#. <i>Sebastian Banescu, Ciprian Lucaci, Benjamin Kraemer and Alexander Pretschner (Technische Universität München)</i>	18.30 – 22.00 Dinner sponsored by NAGRA
Binary Permutation Polynomial Inversion and Application to Obfuscation Techniques. <i>Lucas Barthélémy (Quarkslab and UPMC), Ninon Eyrolles (Quarkslab), Guenaël Renault and Raphaël Roblin (UPMC).</i>	

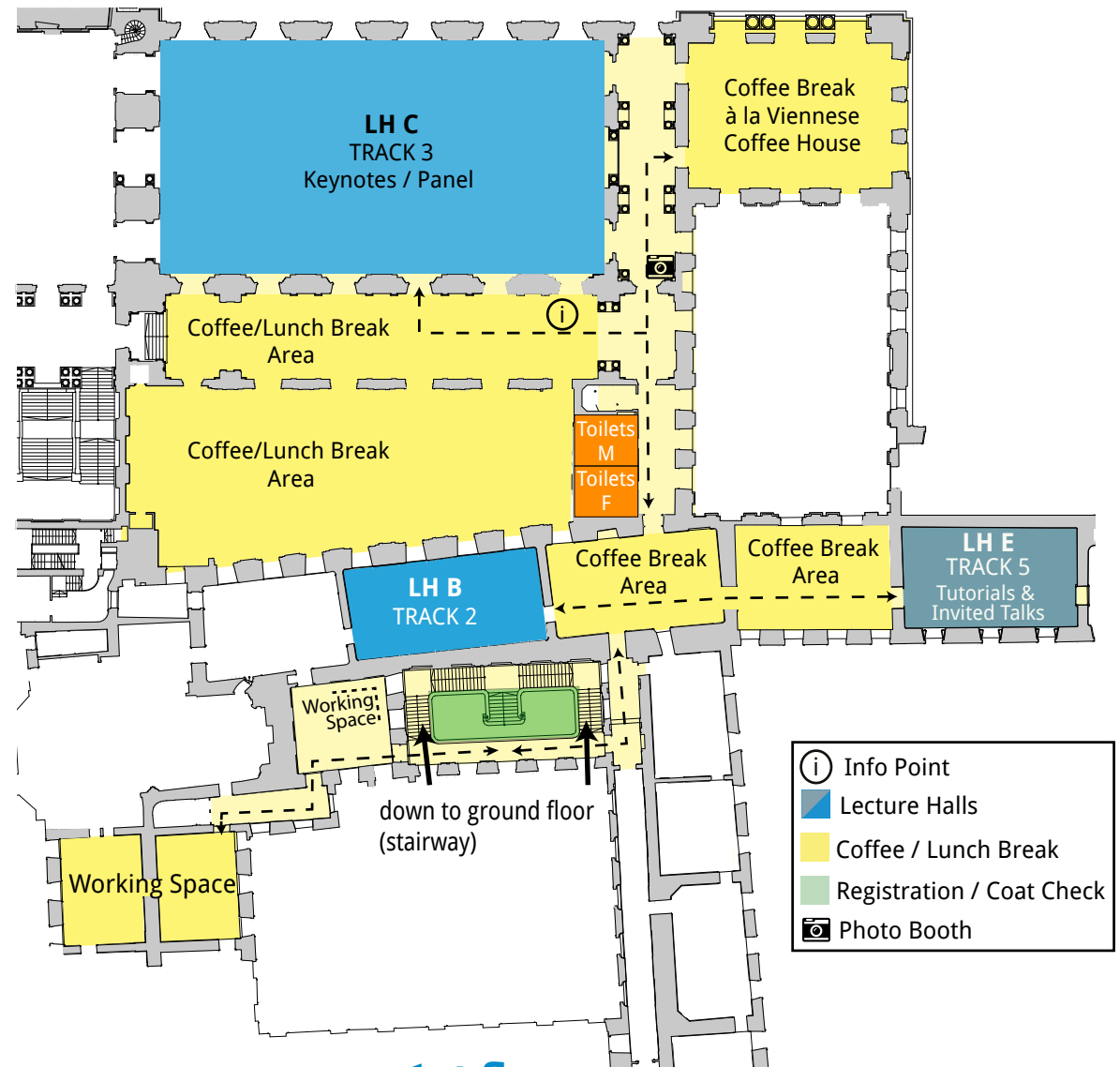
9th ACM Workshop on Artificial Intelligence and Security (AIsEc 2016) Friday, October 28, Lecture Hall J <i>PC Chairs: David Freeman (LinkedIn Corporation, USA) Katerina Mitrokoitsa (Chalmers University of Technology, Sweden) and Arunesh Sinha (University of Michigan, Ann Arbor, USA)</i>	
07.30 – 08.50 Registration & Early Bird Coffee	12.40 – 14.15 Lunch Break
08.50 – 10.00 Welcome and Keynote Keynote: Why is applying machine learning to anti-abuse so hard? <i>Elie Bursztein (Google, Inc., US)</i>	14.15 – 15.30 Session 3: Foundations <i>Session Chair: Brad Miller (Google, Inc., USA)</i> Secure Kernel Machines against Evasion Attacks. <i>Paolo Russu, Ambra Demontis, Battista Biggio, Giorgio Fumera and Fabio Roli (University of Cagliari, Italy)</i>
10.00 – 10.30 Session 1: Security Data Sets <i>Session Chair: David Mandell Freeman (LinkedIn Corporation, USA)</i> SherLock vs Moriarty: A Smartphone Dataset for Cybersecurity Research. <i>Yisroel Mirsky, Asaf Shabtai, Lior Rokach, Bracha Shapira and Yuval Elovici (Ben-Gurion University, Israel)</i>	Prescience: Probabilistic Guidance on the Retraining Conundrum for Malware Detection. <i>Amit Deo, Santanu Dash, Guillermo Suarez-Tangil, Vladimir Vovk and Lorenzo Cavallaro (Royal Holloway, University of London, UK)</i>
10.30 – 11.00 Coffee Break	Discriminative models for multi-instance problems with tree-structure. <i>Tomas Pevný (Czech Technical University in Prague, Czech Republic) and Petr Somol (Cisco Systems, Inc., Czech Republic)</i>
11.00 – 12.40 Session 2: Machine Learning and Security in Practice <i>Session Chair: Battista Biggio (University of Cagliari, Italy)</i> DeepDGA: Adversarially-Tuned Domain Generation and Detection. <i>Hyrum Anderson, Jonathan Woodbridge and Bobby Filar (Endgame, Inc., USA)</i>	15.30 – 16.00 Coffee Break
Tracked Without a Trace: Linking Sessions of Users by Unsupervised Learning of Patterns in Their DNS Traffic. <i>Matthias Kirchler (Humboldt University of Berlin, Germany), Dominik Herrmann, Jens Lindemann (University of Hamburg, Germany) and Marius Kloft (Humboldt University of Berlin, Germany)</i>	16.00 – 17.40 Session 4: Privacy <i>Session Chair: Konrad Rieck (TU Braunschweig, Germany)</i> True Friends Let You Down: Benchmarking Social Graph Anonymization Schemes. <i>Kumar Sharad (University of Cambridge, UK)</i>
Identifying Encrypted Malware Traffic with Contextual Flow Data. <i>Blake Anderson and David McGrew (Cisco Systems Inc., USA)</i>	Change of Guard: The Next Generation of Social Graph De-anonymization Attacks. <i>Kumar Sharad (University of Cambridge, UK)</i>
Causality-based Sensemaking of Network Traffic for Android Application Security. <i>Hao Zhang, Danfeng Yao and Naren Ramakrishnan (Virginia Tech, USA)</i>	Differentially Private Online Active Learning with Applications to Anomaly Detection. <i>Mohsen Ghassemi, Anand Sarwate and Rebecca Wright (Rutgers, The State University of New Jersey, USA)</i>
	A Dual Perturbation Approach for Differential Private ADMM-Based Distributed Empirical Risk Minimization. <i>Tao Zhang and Quanyan Zhu (New York University, USA)</i>
	17.40 – 17.45 Conclusion

Friday, October 28, 2016

main conference



ground floor



1st floor

- (i) Info Point
- Lecture Halls
- Coffee / Lunch Break
- Registration / Coat Check
- 📷 Photo Booth





Please find all details
and further information
in the CCS 2016 Venue Guide:
<http://bit.ly/VenueGuideCCS2016>

General Information

Directions

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](http://www.airportdriver.at). It can be booked online: <http://www.airportdriver.at/en/airport-transfer>.

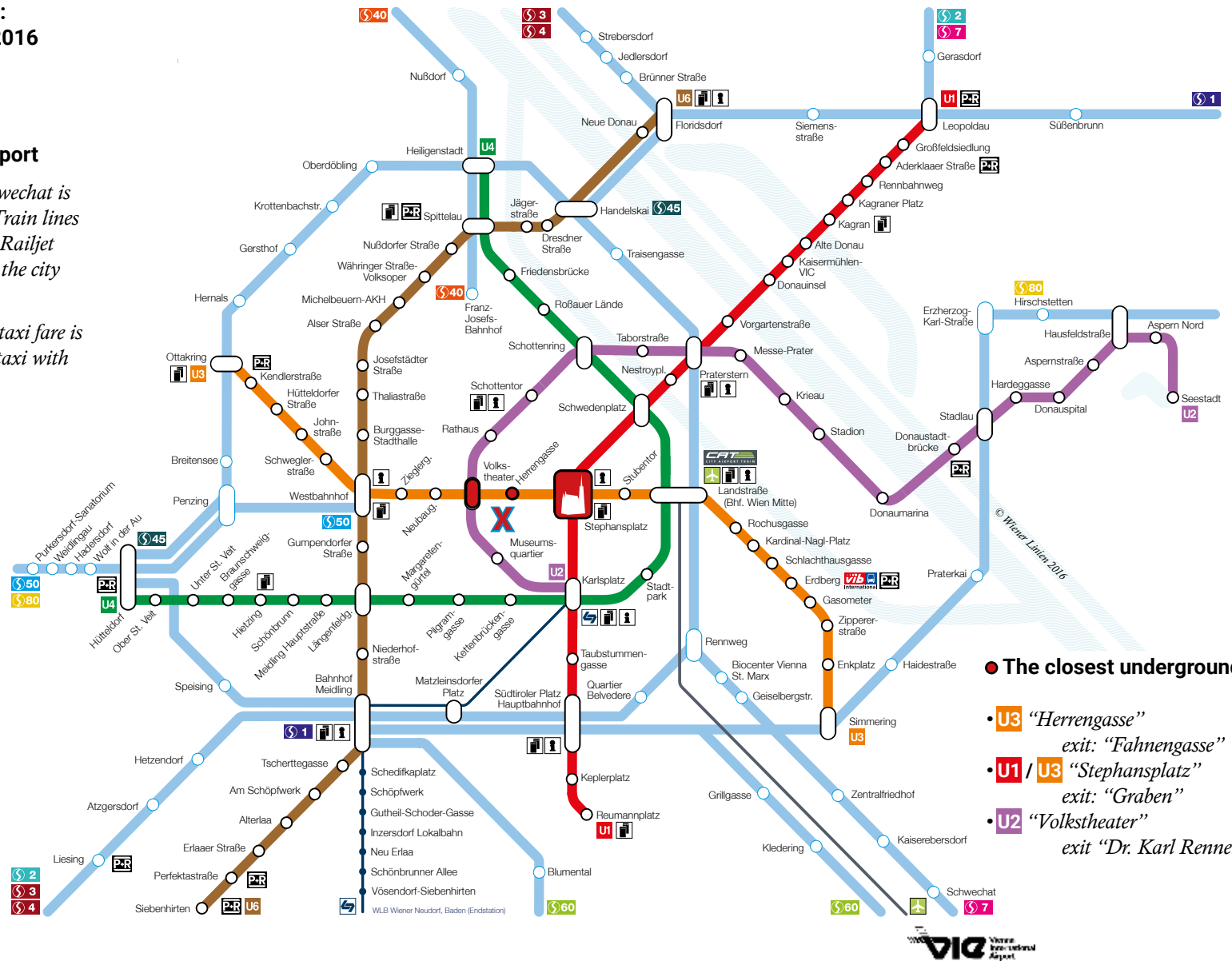
Overview about connections

	CAT	S-Bahn	ICE/ Railjet
Price	11 €	3,9 €	3,9 €
Duration	16 min.	25 min.	18 min.
Connections	Train Station Wien Mitte (U4/U3)	Train Station Wien Mitte (U4/U3)	Main Station (Hauptbahnhof) (U1)

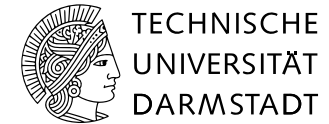
X conference.venue

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

GPS Coordinates:
48.206843, 16.365629



special.thanks



_organization



—platinum.sponsor



_gold.sponsors



Hewlett Packard
Enterprise



IBM Research

_silver.sponsors



_bronze.sponsors

Tuesday, October 25, 2016

	Track 1 Cryptographic Mechanisms	Track 2 Differential Privacy / Cryptography / Attacks	Track 3 Web/Mobile Security	Track 4 Secure Code and Systems	Track 5 Tutorials & Talks
	LH A	LH B	LH C	LH D	LH E
07.30 08.40	Registration & Early Bird Coffee X				
08.40 08.50	Opening @ LH C X				
08.50 09.50	Keynote @ LH C ● Cybersecurity, Nuclear Security, Alan Turing, and Illogical Logic Martin Hellman (Stanford University, US)				
10.00 11.30	Session 1A ●	Session 1B ●	Session 1C ●	Session 1D ●	Tutorial 1 ●
11.30 12.00	Coffee Break ●				
12.00 13.00	Session 2A ●	Session 2B ●	Session 2C ●	Session 2D ●	Invited Talk ●
13.00 14.30	Lunch Break ●				
14.30 16.00	Session 3A ●	Session 3B ●	Session 3C ●	Session 3D ●	Tutorial 2 ●
16.00 16.30	Coffee Break ●				
16.30 18.00	Session 4A ●	Session 4B ●	Session 4C ●	Session 4D ●	Tutorial 2 ●
18.30 23.00	Mayor's Dinner @ Vienna City Hall ● Poster / Demo Session & Award Ceremony				

Wednesday, October 26, 2016

	Track 1 Cryptographic Mechanisms	Track 2 Differential Privacy / Cryptography / Attacks	Track 3 Web/Mobile Security	Track 4 Secure Code and Systems	Track 5 Tutorials & Talks
	LH A	LH B	LH C	LH D	LH E
07.30 08.50	Registration & Early Bird Coffee ●				
08.50 09.50	Keynote @ LH C ● Is it practical to build a truly distributed payment system? Ross Anderson (University of Cambridge, UK)				
10.00 11.30	Session 5A ●	Session 5B ●	Session 5C ●	Session 5D ●	Tutorial 3 ●
11.30 12.00	Coffee Break ●				
12.00 13.00	Session 6A ●	Session 6B ●	Session 6C ●	Session 6D ●	Tutorial 4 12.00-13.15 ●
13.00 14.30	Lunch Break ●				
14.30 16.00	Session 7A ●	Session 7B ●	Session 7C ●	Session 7D ●	Tutorial 5 ●
16.00 16.30	Coffee Break ●				
16.30 18.00	Session 8A ●	Session 8B ●	Session 8C ●	Session 8D ●	Invited Talks ●
18.05 19.00	Panel Discussion @ LH C ● Impact of Academic Security Research: Frogs in Wells, Storms in Teacups, or Raw Diamonds?				
19.00 24.00	Traditional Viennese Dinner @ Heuriger ●				

Thursday, October 27, 2016

	Track 1 Cryptographic Mechanisms	Track 2 Differential Privacy / Cryptography / Attacks	Track 3 Web/Mobile Security	Track 4 Secure Code and Systems	Track 5 Tutorials & Talks
	LH A	LH B	LH C	LH D	LH E
08.15 09.30	Registration & Early Bird Coffee ●				
09.30 11.00	Session 9A 09.00-10.30 ●	Session 9B ●	Session 9C ●	Session 9D ●	
11.00 11.30	Coffee Break ●				
11.30 13.00	Session 10A ●	Session 10B ●	Session 10C ●	Session 10D ●	Tutorial 6 ●
13.00 14.30	Lunch Break ●				
14.30 16.00	Session 11A ●	Session 11B ●	Session 11C ●	Session 11D ●	Tutorial 7 ●
16.00 16.30	Coffee Break				
16.30 18.00	Session 12A ●	Session 12B ●	Session 12C ●	Session 12D ●	Tutorial 7 ●
18.05 19.00	CCS Business Meeting @ LH C ●				
19.15 20.45	Sightseeing ● For ticket holders only! (Window for purchase closed on 21/10/2016)				

SHORT INDEX

LH A
LH B
LH C
LH D
LH E

Lecture Hall A
Lecture Hall B
Lecture Hall C
Lecture Hall D
Lecture Hall E

~~X~~ wanna join
● not sure yet

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



@acm_ccs #ccs16
ssid: CCS_Participants
pwd: ccs4s3curity

www.sigsac.org/ccs/CCS2016