Registration on Sunday Nov 3rd, 2013

16:00-18:00	**Registration – Foyer (Room B02)** *To avoid long waiting lines on Monday and Tuesday, please try to register on Sunday*

Pre-Conference Workshops on Monday, Nov 4th, 2013

Language Support for Privacy-Enhancing Technologies (PETShop) – Room B04 **PC Chairs:** Martin Franz (Deutsche Bank), Andreas Holzer (Vienna University of Technology)	**Trustworthy Embedded Devices (TrustED) – Room B05-B06** **PC Chairs:** Frederik Armknecht (University of Mannheim), Jean-Pierre Seifert (TU Berlin / Deutsche Telekom Laboratories)
07:30 – 08:30: **Breakfast & Registration**	
Welcome (08:50 – 09:00) **Invited Talk (09:00 – 10:00)** A Brief History of Practical Multi-Party Computation. *Nigel Smart (University of Bristol).* **Session 1a: Protocols (10:00 – 10:30)** Specifying Sharemind's Arithmetic Black Box. *Peeter Laud, Alisa Pankova, Martin Pettai, Jaak Randmets.*	**Welcome (08:50 – 09:00)** **Invited Talk (09:00 – 10:00)** Physical Unclonable Functions: Devices for Cryptostorage. *Rainer Plaga.* **Session 1 (10:00 – 10:30)** 10.00-10.30: Machine code verification of a tiny ARM hypervisor. *Mads Dam, Roberto Guanciale, Hamed Nemati.*
10:30 – 11:00: **Coffee Break**	
Session 1b: Protocols (11:00 – 12:30) Domain-Polymorphic Language for Privacy-Preserving Applications. *Dan Bogdanov, Peeter Laud and Jaak Randmets.* Pinocchio Coin: Building Zerocoin from a Succinct Pairing-based Proof System. *George Danezis, Cedric Fournet, Markulf Kohlweiss, Bryan Parno.* Towards an EasyCrypt Formalization of Garbling Schemes. *José Carlos Bacelar Almeida, Manuel Bernardo Barbosa, Gilles Barthe, Guillaume Davy, François Dupressoir, Benjamin Grégoire, Pierre-Yves Strub.*	**Session 2 (11:00 – 12:30)** Bias-based Modeling and Entropy Analysis of PUFs. *Robbert van Den Berg, Boris Skoric, Vincent van der Leest.* Efficient Hardware Implementation of the Stream Cipher WG-16 with Composite Field Arithmetic. *Xinxin Fan, Nusa Zidaric, Mark Aagaard, Guang Gong.* Securing Implantable Cardiac Medical Devices: Use of Radio Frequency Energy Harvesting. *Nourhene Ellouze, Mohamed Allouche, Habib Ben Ahmed, Slim Rekhis, Noureddine Boudriga.*
12:30 – 14:00: **Lunch Break**	
Invited Talk (14:00 – 15:00) Non-Interactive Secure Computation Systems. *Benny Pinkas (Bar Ilan University).* **Session 2a: Compiler (15:00 – 15:30)** Efficient Secure Computation Optimization. *Raphael Urmoneit, Florian Kerschbaum.*	**Session 3 (14:00 – 15:30)** Breaking through Fixed PUF Block Limitations with Differential Sequence Coding and Convolutional Codes. *Matthias Hiller, Michael Weiner, Leandro Rodrigues Lima, Maximilian Birkner, Georg Sigl.* Secure PRNG Seeding on Commercial Of-the-Shelf Microcontrollers. *Anthony Van Herrewege, Vincent van der Leest, Andre Schaller, Stefan Katzenbeisser, Ingrid Verbauwhede.* Securing Data Provenance in Body Area Networks using Lightweight Wireless Link Fingerprints. *Syed Taha Ali, Vijay Sivaraman, Sanjay Jha, Diethelm Ostry.*
15:30 – 16:00: **Coffee Break**	
Session 2b: Compiler (16:00 – 17:00) Lessons Learned with PCF: Scaling Secure Computation. *Benjamin Kreuter, Abhi Shelat.* Challenges in Compiler Construction for Secure Two-Party Computation. *Andreas Holzer, Nikolaos P. Karvelas, Stefan Katzenbeisser, Helmut Veith, Martin Franz.*	**Invited Talk (16:00 – 17:00)** Feasibly Clonable Functions. *Christian Boit.* **Adjourn (17:00 – 17:10)**

Security, Privacy and Dependability for Cyber Vehicles (CyCAR) – Room B95

PC Chairs: Farinaz Koushanfar (Rice University), Albert Held (Daimler AG)
General Chairs: Cliff Wang (Army Research Office), Hervé Seudie (Robert Bosch GmbH)

Artificial Intelligence and Security (AISec) – Room B07-B08

PC Chairs: Blaine Nelson (University of Potsdam), Christos Dimitrakakis (Chalmers University of Technology), Elaine Shi (University of Maryland)

07:30 – 08:30: **Breakfast & Registration**

Keynote (08:30 – 09:30)

Mobility of the Future. *Ulrich Huber.*

Session 1a: In-Car Security Issues and Protocols (09:30 – 10:30)

Practical Information-Flow Aware Middleware for In-Car Communication. *Alexandre Bouard, Benjamin Weyl, Claudia Eckert.*

Efficient and Secure Storage of Private Keys for Pseudonymous Vehicular Communication. *Michael Feiri, Jonathan Petit, Frank Kargl.*

Introduction and Keynote (08:30 - 10:00)

Introduction by *Blaine Nelson.*

Off the Beaten Path: Machine Learning for Offensive Security. *Konrad Rieck.*

10:30 – 11:00: **Coffee Break**

Session 1b: In-Car Security Issues and Protocols (11:00 – 11:30)

Lightweight Secure Communication Protocols for In-Vehicle Sensor Networks. *Miao Xu, Wenyuan Xu, Jesse Walker, Benjamin Moore.*

Session 2a: Security and Privacy Issues in V2X Communication (11:30 – 12:30)

Secure Smartphone-based Registration and Key Deployment for Vehicle-to-Cloud Communications. *Julian Timpner, Dominik Schürmann, Lars Wolf.*

POPCORN: Privacy-Preserving Charging for eMobility. *Christina Hoefer, Jonathan Petit, Robert Schmidt, Frank Kargl.*

Session 1: Security in Societal Computing (10:30 - 12:30)

Using Naive Bayes to Detect Spammy Names in Social Networks. *David Mandell Freeman.*

What You Want Is Not What You Get: Predicting Sharing Policies for Text-based Content on Facebook. *Arunesh Sinha, Yan Li, Lujo Bauer.*

GOTCHA Password Hackers! *Jeremiah Blocki, Manuel Blum, Anupam Datta.*

Early Security Classification of Skype Users via Machine Learning. *Anna Leontjeva, Moises Goldszmidt, Yinglian Xie, Fang Yu, Martín Abadi.*

12:30 – 14:00: **Lunch Break**

Session 2b: Security and Privacy Issues in V2X Communication (14:00 – 14:30)

Trust Assurance Levels of Cybercars in V2X Communication. *Hervé Seudié, Daniel Angermeier, Alexander Kiening, Tyrone Stodardt, Marko Wolf.*

Invited Paper and Invited Talk (14:30 – 15:00)

Hardware and Embedded Security in the Context of Internet of Things. *A. Kanuparthi, S. Addepalli R. Karri.*

Panel Discussions (15:00 – 15:30)

Session 2: Intrusion and Malware Detection (14:00 - 15:30)

Structural Detection of Android Malware using Embedded Call Graphs. *Hugo Gascon, Fabian Yamaguchi, Daniel Arp, Konrad Rieck.*

ACTIDS: An Active Strategy For Detecting and Localizing Network Attacks. *Eitan Menahem, Gabi Nakibly, Nir Amar, Yuval Elovici.*

A Close Look on n-Grams in Intrusion Detection: Anomaly Detection vs. Classification. *Christian Wressnegger, Guido Schwenk, Daniel Arp, Konrad Rieck.*

15:30 – 16:00: **Coffee Break**

Session 3: Adversarial Learning (from 16:00)

On the Hardness of Evading Combinations of Linear Classifiers. *David Stevens, Daniel Lowd.*

Is Data Clustering in Adversarial Settings Secure? *Battista Biggio, Ignazio Pillai, Samuel Rota Bulò, Davide Ariu, Marcello Pelillo, Fabio Roli.*

Approaches to Adversarial Drift. *Alex Kantchelian, Sadia Afroz, Ling Huang, Aylin Caliskan Islam, Brad Miller, Michael Tschantz, Rachel Greenstadt, Anthony Joseph, J.D. Tygar.*

Privacy in the Electronic Society (WPES) – Room C01 & B09

PC Chair: Sara Foresti (Università degli Studi di Milano)

Track A in Room C01	Track B in Room B09
07:30 – 08:25: **Breakfast & Registration**	
08:25 – 08:30: **Opening**	
Session 1A: Privacy in Social Network and Access Control (08.30 - 10.30) The Post Anachronism: The Temporal Dimension of Facebook Privacy. *Lujo Bauer, Lorrie Faith Cranor, Saranga Komanduri, Michelle L. Mazurek, Michael K. Reiter, Manya Sleeper, Blase Ur.* Anonymously Sharing Flickr Pictures with Facebook Friends. *Jan Camenisch, Günter Karjoth, Gregory Neven, Franz-Stefan Preiss.* On the Use of Decentralization to Enable Privacy in Web-Scale Recommendation Services. *Animesh Nandi, Armen Aghasaryan, Ishan Chhabra.* Optimally Private Access Control. *Markulf Kohlweiss, Alfredo Rial.*	**Session 1B: Anonymity (08.30 - 10.30)** You Cannot Hide for Long: De-Anonymization of Real-World Dynamic Behaviour. *George Danezis, Carmela Troncoso.* Analysis of the Impact of Data Granularity on Privacy for the Smart Grid. *Valentin Tudor, Magnus Almgren, Marina Papatriantafilou.* Thinking Inside the BLAC Box: Smarter Protocols for Faster Anonymous Blacklisting. *Ryan Henry, Ian Goldberg.* Distributed Privacy-Preserving Transparency Logging. *Tobias Pulls, Roel Peeters, Karel Wouters.*
10:30 – 11:00: **Coffee Break**	
Session 2A: Privacy of Genomic Data and of Accesses (11.00 - 12.30) Protecting and Evaluating Genomic Privacy in Medical Tests and Personalized Medicine. *Erman Ayday, Jean Louis Raisaro, Jacques Rougemont, Jean-Pierre Hubaux.* Secure Genomic Testing with Size- and Position-Hiding Private Substring Matching. *Emiliano De Cristofaro, Sky Faber, Gene Tsudik.* Outsourced Private Information Retrieval. *Yizhou Huang, Ian Goldberg.*	**Session 2B: Privacy Preserving Computation (11.00 - 12.30)** Distributed ElGamal á la Pedersen - Application to Helios. *Véronique Cortier, David Galindo, Stéphane Glondu, Malika Izabachene.* Privacy-Preserving Billing for e-Ticketing Systems in Public Transportation. *Florian Kerschbaum, Hoon Wei Lim, Ivan Gudymenko.* Canon-MPC, A System for Casual Non-Interactive Secure Multi-Party Computation Using Native Client. *Ayman Jarrous, Benny Pinkas.*
12:30 – 14:00: **Lunch Break**	
Session 3A: Location Privacy (14.00 - 15.30) Optimal Sporadic Location Privacy Preserving Systems in Presence of Bandwidth Constraints. *Michael Herrmann, Carmela Troncoso, Claudia Diaz, Bart Preneel.* Inferring Social Ties in Academic Networks Using Short-Range Wireless Communications. *Igor Bilogrevic, Kévin Huguenin, Murtuza Jadliwala, Florent Lopez, Jean-Pierre Hubaux, Philip Ginzboorg, Valtteri Niemi.* Redeem with Privacy (RwP): Privacy Protecting Framework for Geo-social Commerce. *Md Moniruzzaman, Ken Barker.*	**Session 3B: Anonymous Communication (14.00 - 15.30)** Improved Website Fingerprinting on Tor. *Tao Wang, Ian Goldberg.* ScrambleSuit: A Polymorphic Network Protocol to Circumvent Censorship. *Philipp Winter, Tobias Pulls, Juergen Fuss.* On the Limits of Provable Anonymity. *Nethanel Gelernter, Amir Herzberg.*
15:30 – 16:00: **Coffee Break**	
Session 4A: Privacy Protocols, Password Security, and Privacy in Social Media (16.00 - 17.40) Using Mobile Device Communication to Strengthen E-voting Protocols. *Michael Backes, Martin Gagné, Malte Skoruppa.* Conscript Your Friends into Larger Anonymity Sets with JavaScript. *Henry Corrigan-Gibbs, Bryan Ford.* Improved Group Off-the-Record Messaging. *Hong Liu, Eugene Vasserman, Nicholas Hopper.* The Password Allocation Problem: Strategies for Reusing Passwords Effectively. *Rishab Nithyanand, Rob Johnson.* Proactive Insider Threat Detection Through Social Media: the YouTube Case. *Miltiadis Kandias, Vasilis Stavrou, Nick Bozovic, Dimitris Gritzalis.*	**Session 4B: Identify and Assess Privacy Risks (16.00 - 17.40)** Inferring Trip Destinations From Driving Habits Data. *Rinku Dewri, Prasad Annadata, Wisam Eltarjaman, Ramakrishna Thurimella.* The Place (and Price) Is Right: An Economic Solution to Location Privacy. *Christopher Riederer, Augustin Chaintreau, Jacob Cahan, Vijay Erramilli.* Privacy Awareness about Information Leakage: Who knows what about me? *Delfina Malandrino, Andrea Petta, Vittorio Scarano, Luigi Serra, Raffaele Spinelli, Balachander Krishnamurthy.* SideAuto: Quantitative Information Flow for Side-Channel Leakage in Web Application. *Xujing Huang, Pasquale Malacaria.* No Surprises: Measuring Intrusiveness of Smartphone Applications By Detecting Objective Context Deviations. *Fan Zhang, Fuming Shih, Daniel Weitzner.*

CCS Main Conference Program on Tuesday Nov 5th, 2013

	TRACK A Room C01	TRACK B Room B05-B06	TRACK C Room B09	TUTORIALS/ INV. TALKS Room B07-B08
07:30-08:30	**Breakfast & Registration – Room B01/B02**			
08:30-09:10	**Opening (General Chair, PC Chair, SIGSAC Chair) – Room C01**			
09:10-09:40	**OPENING KEYNOTE – Room C01** *Cyber Security in Germany* **Martin Schallbruch** (Chief Information Officer at the German Federal Ministry of the Interior)			
09:40-10:00	**Coffee Break – Room B01/B02**			
	Session 1-A **Trusted Systems** ***Session Chair*** **Radu Sion**	***Session 1-B*** **How Crypto Breaks** ***Session Chair*** **Volker Roth**	***Session 1-C*** **Malware** ***Session Chair*** **Thorsten Holz**	
10:00-10:30	**A Security Framework for the Analysis and Design of Software Attestation** *Frederik Armknecht (Universität Mannheim, Germany), Ahmad-Reza Sadeghi (Technische Universität Darmstadt/CASED), Steffen Schulz (Intel Corporation), Christian Wachsmann (Intel Collaborative Research Institute for Secure Computing at TU Darmstadt)*	**Rethinking SSL Development in an Appified World** *Sascha Fahl (Leibniz University Hannover), Marian Harbach (Leibniz Universität Hannover), Henning Perl (Leibniz Universität Hannover), Markus Koetter (Leibniz Universität Hannover), Matthew Smith (Leibniz Universität Hannover)*	**A Clinical Study of Risk Factors Related to Malware Infections** *Fanny Lalonde Lévesque (École Polytechnique de Montréal), Jude Nsiempba (École Polytechnique de Montréal), José M. Fernandez (École Polytechnique de Montréal), Sonia Chiasson (Carleton University), Anil Somayaji (Carleton University)*	
10:30-11:00	**OASIS: On Achieving a Sanctuary for Integrity and Secrecy on Untrusted Platforms** *Emmanuel Owusu (Carnegie Mellon University), Jorge Guajardo (Robert Bosch LLC – Research and Technology Center, Pittsburgh, USA), Jonathan McCune (Carnegie Mellon University), Jim Newsome (Carnegie Mellon University), Adrian Perrig (ETH Zurich, CyLab / Carnegie Mellon University), Amit Vasudevan (Carnegie Mellon University)*	**Protocol Misidentification Made Easy with Format-Transforming Encryption** *Kevin P. Dyer (Portland State University), Scott E. Coull (RedJack, LLC.), Thomas Ristenpart (University of Wisconsin-Madison), Thomas Shrimpton (Portland State University)*	**Delta: Automatic Identification of Unknown Web-Based Infection Campaigns** *Kevin Borgolte (UC Santa Barbara), Christopher Kruegel (UC Santa Barbara), Giovanni Vigna (UC Santa Barbara)*	
11:00-11:30	**BIOS Chronomancy: Fixing the Core Root of Trust for Measurement** *John Butterworth (MITRE), Corey Kallenberg (MITRE), Xeno Kovah (MITRE), Amy Herzog (MITRE)*	**An Empirical Study of Cryptographic Misuse in Android Applications** *Manuel Egele (Carnegie Mellon University), David Brumley (Carnegie Mellon University), Yanick Fratantonio (University of California, Santa Barbara), Christopher Kruegel (University of California, Santa Barbara)*	**Beheading Hydras: Performing Effective Botnet Takedowns** *Yacin Nadji (Georgia Institute of Technology), Manos Antonakakis (Damballa Inc.), Roberto Perdisci (University of Georgia), David Dagon (Georgia Institute of Technology), Wenke Lee (Georgia Institute of Technology)*	**INVITED TALK: Vincenzo Iozzo** *From One Ivory Tower to Another: Wish Listing for Filling the Gaps in Information (In)Security*
11:30-12:00	**Flexible and Scalable Digital Signatures in TPM 2.0** *Liqun Chen (HP Labs), Jiangtao Li (Intel Labs)*	**Detecting Stealthy, Distributed SSH Bruteforcing** *Mobin Javed (UC Berkeley), Vern Paxson (UC Berkeley and ICSI)*	**Shady Paths: Leveraging Surfing Crowds to Detect Malicious Web Pages** *Gianluca Stringhini (University of California, Santa Barbara), Christopher Kruegel (University of California, Santa Barbara), Giovanni Vigna (University of California, Santa Barbara)*	

	TRACK A	TRACK B	TRACK C	TUTORIALS/ INV. TALKS
	Room C01	Room B05-B06	Room B09	Room B07-B08
12:00-13:30	**Lunch Break – Room B01/B02**			
	Session 2-A **Passwords** ***Session Chair*** **Rob Johnson**	***Session 2-B*** **Control & Information Flow** ***Session Chair*** **Ninghui Li**	***Session 2-C*** **Storage Security** ***Session Chair*** **Florian Kerschbaum**	
13:30-14:00	**Honeywords: Making Password-Cracking Detectable** *Ari Juels (RSA), Ronald Rivest (MIT)*	**Monitor Integrity Protection with Space Efficiency and Separate Compilation** *Ben Niu (Lehigh University), Gang Tan (Lehigh University)*	**Multi-Cloud Oblivious Storage** *Emil Stefanov (UC Berkeley), Elaine Shi (University of Maryland)*	
14:00-14:30	**Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns** *Sebastian Uellenbeck (Ruhr-University Bochum), Markus Dürmuth (Ruhr-University Bochum), Christopher Wolf (Ruhr-University Bochum), Thorsten Holz (Ruhr-University Bochum)*	**Relational Abstract Interpretation for the Verification of 2-Hypersafety Properties** *Máté Kovács (Technische Universität München), Helmut Seidl (Technische Universität München), Bernd Finkbeiner (Saarland University)*	**Policy-based Secure Deletion** *Christian Cachin (IBM Research – Zurich), Kristiyan Haralambiev (IBM Research – Zurich), Hsu-Chun Hsiao (Carnegie Mellon University), Alessandro Sorniotti (IBM Research – Zurich)*	**TUTORIAL 1: Lecturer: Christof Paar** *Constructive and Destructive Aspects of Embedded Security in the Internet of Things*
14:30-15:00	**Measuring Password Guessability for an Entire University** *Michelle L. Mazurek (Carnegie Mellon University), Saranga Komanduri (Carnegie Mellon University), Timothy Vidas (Carnegie Mellon University), Lujo Bauer (Carnegie Mellon University), Nicolas Christin (Carnegie Mellon University), Lorrie Faith Cranor (Carnegie Mellon University), Patrick Gage Kelley (University of New Mexico), Richard Shay (Carnegie Mellon University), Blase Ur (Carnegie Mellon University)*	**Formal Verification of Information Flow Security for a Simple ARM-Based Separation Kernel** *Mads Dam (KTH), Roberto Guanciale (KTH), Narges Khakpour (CSC, KTH), Hamed Nemati (KTH), Oliver Schwarz (SICS Swedish Institute of Computer Science)*	**Secure Data Deletion from Persistent Media** *Joel Reardon (ETH Zurich), Hubert Ritzdorf (ETH Zurich), David Basin (ETH Zurich), Srdjan Capkun (ETH Zurich)*	
15:00-15:30	**SAuth: Protecting User Accounts from Password Database Leaks** *Georgios Kontaxis (Columbia University), Elias Athanasopoulos (Columbia University), Georgios Portokalidis (Stevens Institute of Technology), Angelos D. Keromytis (Columbia University)*	**ShadowReplica: Efficient Parallelization of Dynamic Data Flow Tracking** *Kangkook Jee (Columbia University), Vasileios P. Kemerlis (Columbia University), Angelos D. Keromytis (Columbia University), Georgios Portokalidis (Stevens Institute of Technology)*	**PoWerStore: Proofs of Writing for Efficient and Robust Storage** *Dan Dobre (NEC Labs Europe), Ghassan Karame (NEC Labs Europe), Wenting Li (NEC Labs Europe), Matthias Majuntke (Capgemini Deutschland), Neeraj Suri (TU Darmstadt), Marko Vukolić (Eurecom)*	
15:30-16:00	**Coffee Break – Room B01/B02**			

	TRACK A	TRACK B	TRACK C	TUTORIALS/ INV. TALKS
	Room C01	Room B05-B06	Room B09	Room B07-B08
	Session 3-A **Oblivious RAM and Oblivious Computation** ***Session Chair*** **Stefan Katzenbeisser**	***Session 3-B*** **Anonymous Channels** ***Session Chair*** **Nicholas Christin**	***Session 3-C*** **Protocol Analysis & Synthesis** ***Session Chair*** **David Basin**	
16:00-16:30	**Path ORAM: An Extremely Simple Oblivious RAM Protocol** *Emil Stefanov (UC Berkeley), Marten van Dijk (University of Connecticut), Elaine Shi (University of Maryland), Christopher Fletcher (MIT), Ling Ren (MIT), Xiangyao Yu (MIT), Srinivas Devadas (MIT)*	**Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries** *Aaron Johnson (U.S. Naval Research Laboratory), Chris Wacek (Georgetown University), Rob Jansen (U.S. Naval Research Laboratory), Micah Sherr (Georgetown University), Paul Syverson (U.S. Naval Research Laboratory)*	**An Analysis of the EMV Channel Establishment Protocol** *Christina Brzuska (Tel Aviv University), Nigel P. Smart (University of Bristol), Bogdan Warinschi (University of Bristol), Gaven J. Watson (University of Bristol)*	**TUTORIAL 1:** **Lecturer:** **Christof Paar** *Constructive and Destructive Aspects of Embedded Security in the Internet of Things*
16:30-17:00	**PHANTOM: Practical Oblivious Computation in a Secure Processor** *Martin Maas (UC Berkeley), Eric Love (UC Berkeley), Emil Stefanov (UC Berkeley), Mohit Tiwari (UT Austin), Elaine Shi (University of Maryland), Krste Asanovic (UC Berkeley), John Kubiatowicz (UC Berkeley), Dawn Song (UC Berkeley)*	**PCTCP: Per-Circuit TCP-over-IPsec Transport for Anonymous Communication Overlay Networks** *Mashael Alsabah (Qatar Computing Research Institute), Ian Goldberg (University of Waterloo)*	**On the Security of TLS Renegotiation** *Florian Giesen (Ruhr-Universität Bochum), Florian Kohlar (Ruhr-Universität Bochum), Douglas Stebila (Queensland University of Technology)*	
17:00-17:30	**Practical Dynamic Proofs of Retrievability** *Elaine Shi (University of Maryland), Emil Stefanov (UC Berkeley), Charalampos Papamanthou (University of Maryland)*	**Cover Your ACKs: Pitfalls of Covert Channel Censorship Circumvention** *John Geddes (University of Minnesota), Maxfield Schuchard (University of Minnesota), Nicholas Hopper (University of Minnesota)*	**Using SMT Solvers to Automate Design Tasks for Encryption and Signature Schemes** *Joseph A. Akinyele (Johns Hopkins University), Matthew Green (Johns Hopkins University), Susan Hohenberger (Johns Hopkins University)*	
17:30-18:30	**PANEL Discussion – Room C01** *Distributed Monitoring and Analytics: Finding the Needle in the Haystack in Real Time* **Moderator: David McGrew (Cisco)**			
18:30-20:30	**Poster Session & Cocktail Reception – Room B01**			

CCS Main Conference Program on Wednesday, Nov 6th, 2013

	TRACK A	TRACK B	TRACK C	TUTORIALS/ INV. TALKS
	Room C01	Room B05-B06	Room B09	Room B07-B08
07:30-08:30	**Breakfast – Room B01/B02**			
08:30-09:30	**KEYNOTE – Room C01** *The Science, Engineering and Business of Cyber Security* **Ravi Sandhu** (Executive Director of the Institute for Cyber Security at the UT San Antonio)			
	Session 4-A **Network Security** ***Session Chair*** **Dongyan Xu**	***Session 4-B*** **Critical Infrastructures** ***Session Chair*** **Klaus Kursawe**	***Session 4-C*** **Attribute-based Encryption** ***Session Chair*** **Liqun Chen**	
09:30-10:00	**AVANT-GUARD: Scalable and Vigilant Switch Flow Management in Software-Defined Networks** *Seungwon Shin (Texas A&M University), Vinod Yegneswaran (SRI International), Phillip Porras (SRI International), Guofei Gu (Texas A&M University)*	**Impact of Integrity Attacks on Real-Time Pricing in Smart Grids** *Rui Tan (Advanced Digital Sciences Center, Illinois at Singapore), Varun Badrinath Krishna (Advanced Digital Sciences Center, Illinois at Singapore), David K. Y. Yau (Advanced Digital Sciences Center, Illinois at Singapore and Singapore Univeristy of Technology and Design), Zbigniew Kalbarczyk (University of Illinois at Urbana-Champaign)*	**Practical Constructions and New Proof Methods for Large Universe Attribute-Based Encryption** *Yannis Rouselakis (University of Texas at Austin), Brent Waters (University of Texas at Austin)*	**TUTORIAL 2: Lecturers: Jan-Erik Ekberg, Kari Kostiainen, N. Asokan** *Trusted Execution Environments on Mobile Devices*
10:00-10:30	**MinimaLT: Minimal-latency Networking Through Better Securit** *Michael Petullo (University of Illinois at Chicago), Jon Solworth (University of Illinois at Chicago), Daniel Bernstein (University of Illinois at Chicago), Tanja Lange (TU Eindhoven), Xu Zhang (University of Illinois at Chicago)*	**Configuration-based IDS for Advanced Metering Infrastructure** *Muhammad Qasim Ali (University of North Carolina at Charlotte), Ehab Al-Shaer (UNCC)*	**Blackbox Traceable CP-ABE: How to Catch People Leaking Their Keys by Selling Decryption Devices on eBay** *Zhen Liu (Shanghai Jiao Tong University, City University of Hong Kong), Zhenfu Cao (Shanghai Jiao Tong University), Duncan Wong (City University of Hong Kong)*	
10:30-11:00	**Coffee Break – Room B01/B02**			
	Session 5-A **Programming Securely** ***Session Chair*** **Jose Fernandez**	***Session 5-B*** **Secure Multiparty Computation** ***Session Chair*** **Michael Waidner**	***Session 5-C*** **Formal Methods** ***Session Chair*** **Claudia Diaz**	
11:00-11:30	**Obfuscation Resilient Binary Code Reuse through Trace-oriented Programming** *Junyuan Zeng (University of Texas at Dallas), Yangchun Fu (University of Texas at Dallas), Kenneth Miller (University of Texas at Dallas), Zhiqiang Lin (University of Texas at Dallas), Xiangyu Zhang (Purdue University), Dongyan Xu (Purdue University)*	**Fast Two-Party Secure Computation with Minimal Assumptions** *Abhi Shelat (University of Virginia), Chih-Hao Shen (University of Virginia)*	**Belief Semantics of Authorization Logic** *Andrew Hirsch (George Washington University), Michael Clarkson (George Washington University)*	

	TRACK A	TRACK B	TRACK C	TUTORIALS/ INV. TALKS
	Room C01	Room B05-B06	Room B09	Room B07-B08
11:30-12:00	**Chucky: Exposing Missing Checks in Source Code for Vulnerability Discovery** *Fabian Yamaguchi (University of Goettingen), Christian Wressnegger (idalab GmbH), Hugo Gascon (University of Goettingen), Konrad Rieck (University of Goettingen)*	**More Efficient Oblivious Transfer and Extensions for Faster Secure Computation** *Gilad Asharov (Bar-Ilan University), Yehuda Lindell (Bar-Ilan University), Thomas Schneider (TU Darmstadt), Michael Zohner (TU Darmstadt)*	**Automatic Verification of Protocols with Lists of Unbounded Length** *Bruno Blanchet (INRIA Paris-Rocquencourt), Miriam Paiola (INRIA Paris-Rocquencourt)*	**TUTORIAL 2: Lecturers: Jan-Erik Ekberg, Kari Kostiainen, N. Asokan** *Trusted Execution Environments on Mobile Devices*
12:00-12:30	**Scheduling Blackbox Mutational Fuzzing** *Maverick Woo (Carnegie Mellon University), Sang Kil Cha (Carnegie Mellon University), Samantha Gottlieb (Carnegie Mellon University), David Brumley (Carnegie Mellon University)*	**An Architecture for Practical Actively Secure MPC with Dishonest Majority** *Marcel Keller (University of Bristol), Peter Scholl (University of Bristol), Nigel Smart (University of Bristol)*	**Relational Abstraction in Community-Based Secure Collaboration** *Philip Fong (University of Calgary), Pooya Mehregan (University of Calgary), Ram Krishnan (University of Texas at San Antonio)*	
12:30-14:00	**Lunch Break – Room B01/B02**			
	Session 6-A **Mobile Security Issues** ***Session Chair*** **Kosta Beznosov**	***Session 6-B*** **Randomness** ***Session Chair*** **Giuseppe Ateniese**	***Session 6-C*** **Hardware Security** ***Session Chair*** **Ruby Lee**	
14:00-14:30	**When Kids Toys Breach Mobile Phone Security** *Abdul Serwadda (Louisiana Tech University), Vir Phoha (Louisiana Tech University)*	**Security Analysis of Pseudo-Random Number Generators with Input: /dev/random is not Robust** *Yevgeniy Dodis (New York University), David Pointcheval (Ecole Normale Superieure), Sylvain Ruhault (Ecole Normale Superieure and Oppida), Damien Vergnaud (Ecole Normale Superieure), Daniel Wichs (Northeastern University)*	**FANCI: Identification of Stealthy Malicious Logic Using Boolean Functional Analysis** *Adam Waksman (Columbia University), Matthew Suozzo (Columbia University), Simha Sethumadhavan (Columbia University)*	
14:30-15:00	**Vetting Undesirable Behaviors in Android Apps with Permission Use Analysis** *Yuan Zhang (Fudan University), Min Yang (Fudan University), Bingquan Xu (Fudan University), Zhemin Yang (Fudan University), Guofei Gu (Texas A&M University), Peng Ning (NC State University), X. Sean Wang (Fudan University), Binyu Zang (Fudan University)*	**Predictability of Android OpenSSL's Pseudo Random Number Generator** *Soo Hyeon Kim (The Attached Institute of ETRI and KOREA Unisversity), Daewan Han (The Attached Institute of ETRI), Dong Hoon Lee (KOREA University)*	**Security Analysis of Integrated Circuit Camouflaging** *Jeyavijayan Rajendran (Polytechnic Institute of NYU), Michael Sam (Polytechnic Insitute of NYU), Ozgur Sinanoglu (New York University Abu Dhabi), Ramesh Karri (Polytechnic institute of NYU)*	

	TRACK A	TRACK B	TRACK C	TUTORIALS/ INV. TALKS
	Room C01	Room B05-B06	Room B09	Room B07-B08
15:00-15:30	**The Impact of Vendor Customizations on Android Security** *Lei Wu (North Carolina State University), Michael Grace (North Carolina State University), Yajin Zhou (North Carolina State University), Chiachih Wu (North Carolina State University), Xuxian Jiang (North Carolina State University)*	**Delegatable Pseudorandom Functions and Applications** *Aggelos Kiayias (National and Kapodistrian University of Athens), Stavros Papadopoulos (University of Science & Technology, Hong Kong), Nikos Triandopoulos (RSA Laboratories and Boston University), Thomas Zacharias (National and Kapodistrian University of Athens)*	**Low-Fat Pointers: Compact Encoding and Efficient Gate-Level Implementation of Fat Pointers for Spatial Safety and Capability-based Security** *Albert Kwon (University of Pennsylvania, Philadelphia), Udit Dhawan (University of Pennsylvania, Philadelphia), Jonathan Smith (University of Pennsylvania, Philadelphia), Thomas Knight (BAE Systems), Andre Dehon (University of Pennsylvania, Philadelphia)*	**INVITED TALK: Ivan Martinovic** *Fasten Your Seatbelts – An Overview and Security Considerations of Next Generation Air Traffic Communi-cation*
15:30-16:00	**Unauthorized Origin Crossing on Mobile Platforms: Threats and Mitigation** *Rui Wang (Microsoft Research), Luyi Xing (Indiana University), Xiaofeng Wang (Indiana University), Shuo Chen (Microsoft Research)*	**Ensuring High-Quality Randomness in Cryptographic Key Generation** *Henry Corrigan-Gibbs (Stanford University), Wendy Mu (Stanford University), Dan Boneh (Stanford University), Bryan Ford (Yale University)*	**Breaking and Entering through the Silicon** *Clemens Helfmeier (Semiconductor Devices, TU Berlin), Dmitry Nedospasov (Security in Telecommunications, TU Berlin), Christopher Tarnovsky (IOActive Inc.), Jan Krissler (Security in Telecommunications, TU Berlin), Christian Boit (Semiconductor Devices, TU Berlin), Jean-Pierre Seifert (Security in Telecommunications, TU Berlin)*	
16:00-16:30	**Coffee Break – Room B01/B02**			
	Session 7-A **Web Attacks** ***Session Chair*** **Sotiris Ioannidis**	***Session 7-B*** **Privacy-Preserving Protocols** ***Session Chair*** **Thomas Schneider**	***Session 7-C*** **Systems' Attack Mitigation** ***Session Chair*** **Weidong Cui**	
16:30-17:00	**Polyglots: Crossing Origins by Crossing Formats** *Jonas Magazinius (Chalmers University of Technology), Billy Rios (Google), Andrei Sabelfeld (Chalmers University of Technology)*	**When Private Set Intersection Meets Big Data: An Efficient and Scalable Protocol** *Changyu Dong (University of Strathclyde), Liqun Chen (Hewlett-Packard Laboratories), Zikai Wen (University of Strathclyde)*	**Düppel: Retrofitting Commodity Operating Systems to Mitigate Cache Side Channels in the Cloud** *Yinqian Zhang (University of North Carolina at Chapel Hill), Michael Reiter (University of North Carolina at Chapel Hill)*	**INVITED TALK: Jacob Appelbaum** *The New Threat Models*
17:00-17:30	**Catching Click-Spam in Search Ad Networks** *Vacha Dave (UC San Diego), Saikat Guha (Microsoft Research India), Yin Zhang (The University of Texas at Austin)*	**Privacy-Preserving Matrix Factorization** *Valeria Nikolaenko (Stanford), Stratis Ioannidis (Technicolor), Udi Weinsberg (Technicolor), Marc Joye (Technicolor), Nina Taft (Technicolor), Dan Boneh (Stanford)*	**Tappan Zee (North) Bridge: Mining Memory Accesses for Introspection** *Brendan Dolan-Gavitt (Georgia Institute of Technology), Tim Leek (MIT Lincoln Laboratory), Josh Hodosh (MIT Lincoln Laboratory), Wenke Lee (Georgia Institute of Technology)*	

	TRACK A	TRACK B	TRACK C	TUTORIALS/ INV. TALKS
	Room C01	Room B05-B06	Room B09	Room B07-B08
17:30-18:00	**mXSS Attacks: Attacking well-secured Web-Applications by using innerHTML Mutations** *Mario Heiderich (Ruhr-Universität Bochum), Jörg Schwenk (Ruhr-Universität Bochum), Tilman Frosch (Ruhr-Universität Bochum), Jonas Magazinius (Chalmers University of Technology), Edward Z. Yang (Stanford University)*	**PICCO: A General-Purpose Compiler for Private Distributed Computation** *Yihua Zhang (University of Notre Dame), Aaron Steele (University of Notre Dame), Marina Blanton (University of Notre Dame)*	**Towards Reducing the Attack Surface of Software Backdoors** *Felix Schuster (Ruhr-Universität Bochum), Thorsten Holz (Ruhr-Universität Bochum)*	
18:00-18:45	**Award Ceremony and Announcements – Room C01**			
19:00-19:30	**Bus Transfer to Wasserwerk (30 minutes)**			
20:00-00:00	**Gala Dinner at Wasserwerk**			

CCS Main Conference Program on Thursday, Nov 7th, 2013

	TRACK A	TRACK B	TRACK C	TUTORIALS/ INV. TALKS
	Room C01	Room B05-B06	Room B09	Room B07-B08
07:30-08:30	**Breakfast – Room B01/B02**			
	Session 8-A **Secure Outsourcing Protocols** ***Session Chair*** **Bryan Parno**	***Session 8-B*** **Privacy Models** ***Session Chair*** **George Danezis**	***Session 8-C*** **Be Aware & Beware** ***Session Chair*** **Ari Juels**	
08:30-09:00	**Verifiable Delegation of Computation on Outsourced Data** *Michael Backes (Saarland University and Max Planck Institute for Software Systems), Dario Fiore (Max Planck Institute for Software Systems), Raphael M. Reischuk (Saarland University)*	**Membership Privacy: A Unifying Framework For Privacy Definitions** *Ninghui Li (Purdue University), Wahbeh Qardaji (Purdue University), Dong Su (Purdue University), Yi Wu (Purdue University), Weining Yang (Purdue University)*	**Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education** *Tamara Denning (University of Washington), Adam Lerner (University of Washington), Adam Shostack, Tadayoshi Kohno (University of Washington)*	
09:00-09:30	**Outsourced Symmetric Private Information Retrieval** *Stanislaw Jarecki (University of California, Irvine), Charanjit Jutla (IBM T.J. Watson Research Center), Hugo Krawczyk (IBM), Marcel C. Rosu (IBM T.J. Watson), Michael Steiner (IBM Research)*	**Geo-Indistinguishability: Differential Privacy for Location-Based Systems** *Miguel E. Andres (École Polytechnique), Nicolás E. Bordenabe (INRIA and École Polytechnique), Konstantinos Chatzikokolakis (CNRS and École Polytechnique), Catuscia Palamidessi (INRIA and École Polytechnique)*	**Security Analysis of a Widely Deployed Locking System** *Michael Weiner (Technische Universität München), Maurice Massar (Technische Universität Kaiserslautern), Erik Tews (Technische Universität Darmstadt), Dennis Giese (Technische Universität Darmstadt), Wolfgang Wieser (Ludwig-Maximilians-Universität München)*	
09:30-10:30	**KEYNOTE – Room C01** *The Arms Race* **Mikko Hypponen** (Chief Research Officer of F-Secure)			
10:30-11:00	**Coffee Break – Room B01/B02**			
	Session 9-A **Crypto Tools** ***Session Chair*** **Frederik Armknecht**	***Session 9-B*** **Audit & Code Randomization** ***Session Chair*** **Simha Sethumadavan**	***Session 9-C*** **Mobile Privacy** ***Session Chair*** **Lujo Bauer**	
11:00-11:30	**How to Keep a Secret: Leakage Deterring Public-key Cryptosystems** *Aggelos Kiayias (National and Kapodistrian University of Athens and University of Connecticut), Qiang Tang (National and Kapodistrian University of Athens and University of Connecticut)*	**ASIST: Architectural Support for Instruction Set Randomization** *Antonis Papadogiannakis (Institute of Computer Science, Foundation for Research and Technology – Hellas), Laertis Loutsis (Institute of Computer Science, Foundation for Research and Technology – Hellas), Vassilis Papaefstathiou (Institute of Computer Science, Foundation for Research and Technology – Hellas), Sotiris Ioannidis (Institute of Computer Science, Foundation for Research and Technology – Hellas)*	**Identity, Location, Disease and More: Inferring Your Secrets from Android Public Resources** *Xiaoyong Zhou (Indiana University, Bloomington), Soteris Demetriou (University of Illinois at Urbana-Champaign), Dongjing He (University of Illinois at Urbana-Champaign), Muhammad Naveed (University of Illinois at Urbana-Champaign), Xiaorui Pan (Indiana University, Bloomington), Xiaofeng Wang (Indiana University, Bloomington), Carl Gunter (University of Illinois at Urbana-Champaign), Klara Nahrstedt (University of Illinois at Urbana-Champaign)*	

	TRACK A	TRACK B	TRACK C	TUTORIALS/ INV. TALKS
	Room C01	Room B05-B06	Room B09	Room B07-B08
11:30-12:00	**Zero-Knowledge Using Garbled Circuits: How To Prove Non-Algebraic Statements Efficiently** *Marek Jawurek (SAP Research), Florian Kerschbaum (SAP Research), Claudio Orlandi (Aarhus University)*	**librando: Transparent Code Randomization for Just-in-Time Compilers** *Andrei Homescu (University of California Irvine), Stefan Brunthaler (University of California, Irvine), Per Larsen (University of California, Irvine), Michael Franz (University of California, Irvine)*	**Preventing Accidental Data Disclosure in Modern Operating Systems** *Adwait Nadkarni (North Carolina State University), William Enck (North Carolina State University)*	**INVITED TALK: Felix 'FX' Lindner** *Resistance is Not Futile – Fighting Nation-State Actors and the Borg*
12:00-12:30	**Elligator: Elliptic-Curve Points Indistinguishable from Uniform Random Strings** *Daniel Bernstein (University of Illinois at Chicago), Mike Hamburg (Cryptography Research), Anna Krasnova (RU Nijmegen), Tanja Lange (Technische Universiteit Eindhoven)*	**LogGC: Garbage Collecting Audit Log** *Kyu Hyung Lee (Purdue University), Xiangyu Zhang (Purdue University), Dongyan Xu (Purdue University)*	**AppIntent: Analyzing Sensitive Data Transmission in Android for Privacy Leakage Detection** *Zhemin Yang (Fudan University), Min Yang (Fudan University), Yuan Zhang (Fudan University), Guofei Gu (Texas A&M University), Peng Ning (NC State University), X. Sean Wang (Fudan University)*	
12:30-14:00	**Lunch Break – Room B01/B02**			
	Session 10-A **Graphics, Vision & Security** ***Session Chair*** **N. Asokan**	***Session 10-B*** **Authentication** ***Session Chair*** **Srdjan Capkun**	***Session 10-C*** **Privacy Issues** ***Session Chair*** **Nick Hopper**	
14:00-14:30	**Cross-Origin Pixel Stealing: Timing Attacks Using CSS Filters** *Robert Kotcher (Carnegie Mellon University), Yutong Pei (Carnegie Mellon University), Pranjal Jumde (Carnegie Mellon University), Collin Jackson (Carnegie Mellon University)*	**Anonymous Credentials Light** *Foteini Baldimtsi (Brown University), Anna Lysyanskaya (Brown University)*	**FPDetective: Dusting the Web for Fingerprinters** *Gunes Acar (KU Leuven), Marc Juarez (Institut d'Investigació en Intel-ligència Artificial and KU Leuven), Nick Nikiforakis (KU Leuven), Claudia Diaz (KU Leuven), Seda Gurses (New York University and KU Leuven), Frank Piessens (KU Leuven), Bart Preneel (KU Leuven)*	**TUTORIAL 3: Lecturer: Eric Bodden** *Easily Instrumenting Android Applications for Security Purposes*
14:30-15:00	**Seeing Double: Reconstructing Obscured Typed Input from Repeated Compromising Reflections** *Yi Xu (University of North Carolina at Chapel Hill), Jared Heinly (University of North Carolina at Chapel Hill), Andrew White (University of North Carolina at Chapel Hill), Jan-Michael Frahm (University of North Carolina at Chapel Hill), Fabian Monrose (University of North Carolina at Chapel Hill)*	**Heart-to-Heart (H2H): Authentication for Implanted Medical Devices** *Masoud Rostami (ECE Dept, Rice University), Ari Juels (RSA Laboratories), Farinaz Koushanfar (Rice University)*	**Addressing the Concerns of the Lacks Family: Quantification of Kin Genomic Privacy** *Mathias Humbert (EPFL), Erman Ayday (EPFL), Jean-Pierre Hubaux (EPFL), Amalio Telenti (Institute of Microbiology, University Hospital and University of Lausanne)*	
15:00-15:30	**The Robustness of Hollow CAPTCHAs** *Haichang Gao (Xidian University), Wei Wang (Xidian University), Jiao Qi (Xidian University), Xuqin Wang (Xidian University), Xiyang Liu (Xidian University), Jeff Yan (Newcastle University)*	**OAKE: A New Family of Implicitly Authenticated Diffie-Hellman Protocols** *Andrew C. Yao (IIIS, Tsinghua University, Beijing, China), Yunlei Zhao (Software School, Fudan University, Shanghai, China)*	**Hang with Your Buddies to Resist Intersection Attacks** *David Wolinsky (Yale University), Ewa Syta (Yale University), Bryan Ford (Yale University)*	

	TRACK A	TRACK B	TRACK C	TUTORIALS/ INV. TALKS
	Room C01	Room B05-B06	Room B09	Room B07-B08
15:30-16:00	Coffee Break – Room B01/B02			
	Session 11-A Web and Code Security *Session Chair* Amir Herzberg	*Session 11-B* Crypto Symbolic Analysis *Session Chair* Bruno Blanchet	*Session 11-C* Security/Cryptographic Utilities *Session Chair* Matthew Smith	
16:00-16:30	**Content-Based Isolation: Rethinking Isolation Policy Design on Client Systems** *Alexander Moshchuk (Microsoft Research), Helen Wang (Microsoft Research), Yunxin Liu (Microsoft Research Asia)*	**Certified Computer-Aided Cryptography: Efficient Provably Secure Machine Code from High-Level Implementations** *José Bacelar Almeida (HASLab, INESC TEC and Universidade do Minho), Manuel Barbosa (HASLab, INESC TEC and Universidade do Minho), Gilles Barthe (IMDEA Software Institute), François Dupressoir (IMDEA Software Institute)*	**Efficient Targeted Key Subset Retrieval in Fractal Hash Sequences** *Kelsey Cairns (Washington State University), Thoshitha Gamage (Washington State University), Carl Hauser (Washington State University)*	**TUTORIAL 3:** **Lecturer:** **Eric Bodden** *Easily Instrumenting Android Applications for Security Purposes*
16:30-17:00	**Diglossia: Detecting Code Injection Attacks With Precision and Efficiency** *Sooel Son (The University of Texas at Austin), Kathryn McKinley (Microsoft Research and The University of Texas at Austin), Vitaly Shmatikov (The University of Texas at Austin)*	**Computationally Complete Symbolic Attacker and Key Exchange** *Gergei Bana (INRIA, Paris), Koji Hasebe (University of Tsukuba), Mitsuhiro Okada (Keio University)*	**HIFS: History Independence for File Systems** *Sumeet Bajaj (Stony Brook University), Radu Sion (Stony Brook University)*	
17:00-17:30	**25 Million Flows Later – Large-scale Detection of DOM-based XSS** *Sebastian Lekies (SAP AG), Ben Stock (Friedrich-Alexander-University Erlangen-Nuremberg), Martin Johns (SAP AG)*	**Fully Automated Analysis of Padding-Based Encryption in the Computational Model** *Gilles Barthe (IMDEA Software Institute), Juan Manuel Crespo (IMDEA Software Institute), Benjamin Gregoire (INRIA Sophia-Antipolis), César Kunz (IMDEA Software Institute), Yassine Lakhnech (Université de Grenoble, VERIMAG), Benedikt Schmidt (IMDEA Software Institute), Santiago Zanella-Béguelin (Microsoft Research)*	**AUTOCRYPT: Enabling Homomorphic Computation On Servers To Protect Sensitive Web Content** *Shruti Tople (National University of Singapore), Shweta Shinde (National University of Singapore), Prateek Saxena (National University of Singapore), Zhaofeng Chen (National University of Singapore)*	
17:30-18:00	**deDacota: Toward Preventing Server-Side XSS via Automatic Code and Data Separation** *Adam Doupe (University of California, Santa Barbara), Weidong Cui (Microsoft Research), Mariusz Jakubowski (Microsoft Research), Marcus Peinado (Microsoft Research), Christopher Kruegel (University of California, Santa Barbara), Giovanni Vigna (University of California, Santa Barbara)*	**Deduction Soundness: Prove One, Get Five for Free** *Florian Böhl (Karlsruhe Institute of Technology), Véronique Cortier (LORIA – CNRS), Bogdan Warinschi (University of Bristol)*	**Protecting Sensitive Web Content from Client-side Vulnerabilities with Cryptons** *Xinshu Dong (National University of Singapore), Zhaofeng Chen (Peking University), Hossein Siadati (Polytechnic Institute of New York University), Shruti Tople (National University of Singapore), Prateek Saxena (National University of Singapore), Zhenkai Liang (National University of Singapore)*	
18:00-18:20	Closing Remarks – Room C01			

Post-Conference Workshops on Friday, Nov 8th, 2013

Cloud Computing Security Workshop (CCSW) – Room C01 **PC Chairs**: Ari Juels (RSA Labs), Bryan Parno (Microsoft Research)	**Digital Identity Management (DIM) – Room B05-B06** **PC Chairs:** Thomas Groß (Newcastle University), Marit Hansen (ULD)
07:30 – 08:25: **Breakfast & Registration**	07:30 – 08:30: **Breakfast & Registration**
Welcome (08:25 – 08:30) **Session 1: Code Execution (08:30 – 09:30)** A Versatile Code Execution Isolation Framework with Security First. *Johannes Krude, Ulrike Meyer.* An Architecture for Concurrent Execution of Secure Environments in Clouds. *Ramya Jayaram Masti, Claudio Marforio, Srdjan Capkun.* Generalized External Interaction with Tamper-Resistant Hardware with Bounded Information. *Xiangyao Yu, Christopher Fletcher, Ling Ren, Marten Van Dijk, Srini Devadas.* **Keynote I (09:30 – 10:30)** Challenges of Transforming Swamps Into Clouds. *Slava Kavsan (Microsoft).*	**Session 1: Welcome and Keynote (08:30 – 09:15)** Welcome by *Thomas Groß, Marit Hansen* Keynote: Meanings of "Privacy" in Privacy Enhancing Technologies. *Claudia Díaz.* **Session 2: Cryptographic Methods (09:15 – 10:30)** Universally Composable Adaptive Oblivious Transfer (with Access Control) from Standard Assumptions. *Masayuki Abe, Jan Camenisch, Maria Dubovitskaya, Ryo Nishimaki.* A Secure Channel for Attribute-Based Credentials. *Gergely Alpar, Jaap-Henk Hoepman.* UbiKiMa: Ubiquitous Authentication Using a Smartphone, Migrating from Passwords to Strong Cryptography. *Maarten Everts, Jaap-Henk Hoepman, Johanneke Siljee.*
10:30 – 11.00: **Coffee Break**	
Session 2: Storage (11:00 – 11:40) Authenticated Storage Using Small Trusted Hardware. *Hsin-Jung Yang, Victor Costan, Nickolai Zeldovich, Srini Devadas.* Cloudsweeper: Enabling Data-Centric Document Management for Secure Cloud Archives. *Chris Kanich, Peter Snyder.* **Keynote II (11:40 – 12:40)** *Dr. Marni Dekker (ENISA)*	**Session 3: Human Factors and Socio-Economic Aspects (11:00 – 12:30)** A Comparison of Users' Perceptions of and Willingness to Use Google, Facebook, and Google+ Single-Sign-On Functionality. *Lujo Bauer, Cristian Bravo-Lillo, Elli Fragkaki, William Melicher.* Taboos and Desires of the UK Public for Identity Management in the Future; General Findings from Two Survey Games. *Liesbet van Zoonen, Georgina Turner.* Probing Identity Management – Preliminary Findings. *Lilia Gomez Flores, Sandra Wilson, Dougie Kinnear.*
12:40 – 14:00: **Lunch Break**	12:30 – 14:00: **Lunch Break**
Session 3: Cryptographic Protocols (14:00 – 15:20) On the (Im)possibility of Privately Outsourcing Linear Programming. *Peeter Laud, Alisa Pankova.* Secure Pattern Matching using Somewhat Homomorphic Encryption. *Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, Kazuhiro Yokoyama and Takeshi Koshiba.* Supporting Complex Queries and Access Policies for Multi-user Encrypted Databases. *Muhammad Rizwan Asghar, Giovanni Russello, Bruno Crispo.* Beyond the Ideal Object: Towards Disclosure-Resilient Order-Preserving Encryption Schemes. *Sander Wozniak, Michael Rossberg, Sascha Grau, Ali Alshawish, Guenter Schaefer.*	**Session 4: Security Considerations (14:00 – 15:30)** Geo-Location Based QR-Code Authentication Scheme to Defeat Active Real-Time Phishing Attack. *Seung-Hyun Kim, Sung Hoon Lee, Daeseon Choi, Seung-Hun Jin.* Towards Standardizing Trusted Evidence of Identity. *Bian Yang, Christoph Busch, Julien Bringer, Els Kindt, Ronald Belser, Uwe Seidel, Edward Springmann, Uwe Rabeler, Andreas Wolf, Magnar Aukrust.* Reachability Analysis for Role-Based Administration of Attributes. *Xin Jin, Ram Krishnan, Ravi Sandhu.*
15:20 – 16:00: **Coffee Break**	15:30 – 16:00: **Coffee Break**
Keynote III (16:00 – 17:00) Accountability in the Cloud: Research Challenges and Opportunities. *Dr. Jesus Luna (Research Director, CSA EMEA).* **Session 4: Infrastructure (17:00 – 17:40)** Structural Cloud Audits that Protect Private Information. *Hongda Xiao, Bryan Ford, Joan Feigenbaum.* Cloudoscopy: Services Discovery and Topology Mapping. *Amir Herzberg, Haya Shulman, Johanna Ullrich, Edgar Weippl.*	**Session 5: eIDs and Identity Management (16:00 – 18:00)** Options for Integrating eID and SAML. *Detlef Hühnlein, Jörg Schwenk, Tobias Wich, Florian Feldmann, Vladislav Mladenov, Andreas Mayer, Moritz Horsch, Bud Brügger, Johannes Schmölz.* Federated Identity to Access e-Government Services – Are Citizens Ready for This? *Angela Sasse, Sacha Brostoff, Charlene Jennett, Miguel Malheiros.* **Panel "Future of eIDs and Identity Management"** Moderator: *Thomas Groß.*

Security and Privacy in Smartphones and Mobile Devices (SPSM) – Room B09

PC Chairs: N. Asokan (Aalto University and University of Helsinki), Adrienne Porter Felt (Google)
General Chair: William Enck (North Carolina State University)

Smart Energy Grid Security Workshop (SEGS) – Room B07-B08

PC Chair: Klaus Kursawe (ENCS, Netherlands)

07:30 – 08:30: **Breakfast & Registration**

Welcome (8:30 - 8:35)

N. Asokan (PC Chair)

Keynote (8:35 - 09:45)

Security Composition in the Real World: Squaring the Circle of Mobile Security with Contemporary Device Economics. *Jon Geater (Trustonic).*

Session 1: Platform Hardening (09:45 - 10:30)

Deadbolt: Locking Down Android Disk Encryption. *Adam Skillen, David Barrera, Paul C. Van Oorschot.*

Native Code Execution Control for Attack Mitigation on Android. *Rafael Fedler, Marcel Kulicke, Julian Schütte.*

Session 1: Smart Grid Standards & Protocols (8:30 – 09:45)

A Security Protocol for Information-Centric Networking in Smart Grids. *Bárbara Vieira, Erik Poll.*

DLMS/COSEM Security Level Enhancement to Construct Secure Advanced Metering Infrastructure. *Jaeduck Choi, Incheol Shin.*

Securing ZigBee Smart Energy Profile 1.x with OpenECC Library. *Xinxin Fan, Guang Gong*.

Invited Talk (09:45 – 10:30)

The Future of Smart Grids. *Erwin Kooi.*

10:30 – 11.00: **Coffee Break**

Session 2: Malware Detection (11:00 - 12:30)

Sound and Precise Malware Analysis for Android via Pushdown Reachability and Entry-Point Saturation. *Shuying Liang, Andrew Keep, Matthew Might, David Van Horn, Steven Lyde, Thomas Gilray, Petey Aldous.*

The Curse of 140 Characters: Evaluating The Efficacy of SMS Spam Detection on Android. *Akshay Narayan, Prateek Saxena.*

This Network is Infected: HosTaGe - a Low-Interaction Honeypot for Mobile Devices. *Emmanouil Vasilomanolakis, Shankar Karuppayah, Mathias Fischer, Max Muhlhauser, Mihai Plasoianu, Wulf Pfeiffer, Lars Pandikow.*

AndroTotal: A Flexible, Scalable Toolbox and Service for Testing Mobile Malware Detectors. *Federico Maggi, Andrea Valdi, Stefano Zanero.*

Session 2: Monitoring (11:00 – 12:30)

Detecting Intrusions in Encrypted Control Traffic. *Maarten Hoeve.*

Semantic Security Analysis of SCADA Networks to Detect Malicious Control Commands in Power Grids. *Hui Lin, Adam Slagell, Zbigniew Kalbarczyk, Peter Sauer, Ravishankar Iyer.*

A Distributed Monitoring Architecture for AMIs: Minimizing the Number of Monitoring Nodes and Enabling Collided Packet Recovery. *Incheol Shin, Jun Ho Huh, Yuseok Jeon, David M. Nicol.*

12:30 – 14:00: **Lunch Break**

Session 3: Attacks (14:00 - 14:50)

Sleeping Android: The Danger of Dormant Permissions. *James Sellwood, Jason Crampton.*

PIN Skimmer: Inferring PINs Through The Camera and Microphone. *Laurent Simon, Ross Anderson.*

Session 4: Privacy (14:50 - 15:30)

A Case of Collusion: A Study of the Interface Between Ad Libraries and their Apps. *Theodore Book, Dan Wallach.*

Please Slow Down! The Impact on Tor Performance from Mobility. *Stephen Doswell, Nauman Aslam, David Kendall, Graham Sexton.*

Session 3: Data Protection & Privacy (14:00 – 15:30)

Protection of Consumer Data in the Smart Grid Compliant with the German Smart Metering Guideline. *Anna Biselli, Elke Franz, Maurílio Pereira Coutinho.*

Customer-Centric Energy Usage Data Management and Sharing in Smart Grid Systems. *Gaurav Lahoti, Daisuke Mashima, Wei-Peng Chen.*

Implementation of Privacy Friendly Aggregation for the Smart Grid. *Benessa Defend and Klaus Kursawe.*

Smart Meter Aggregation via Secret-Sharing. *George Danezis, Cedric Fournet, Markulf Kohlweiss, Santiago Zanella-Béguelin.*

15:30 – 16:00: **Coffee Break**

Session 5: Authentication (16:00 - 17:00)

Secure Enrollment and Practical Migration for Mobile Trusted Execution Environments. *Claudio Marforio, Nikolaos Karapanos, Claudio Soriente, Kari Kostiainen, Srdjan Capkun.*

Securitas: User Identification through RGB-NIR Camera Pair on Mobile Devices. *Shijia Pan, An Chen, Pei Zhang.*

Passwords and Interfaces: Towards Creating Stronger Passwords by Using Mobile Phone Handsets. *S M Taiabul Haque, Matthew Wright, Shannon Scielzo.*

Closing Remarks (17:00 – 17:05) by William Enck (General Chair)

Formal Descriptions & Panel Discussion (16:00 – 17:40)

A Formal Model for Sustainable Vehicle-to-Grid Management. *Mohammad Rahman, Fadi Mohsen, Ehab Al-Shaer.*

Toward a Cyber-Physical Topology Language. *Gabriel Weaver, Carmen Cheh, Edmond Rogers, William Sanders, Dennis Gammel.*

Panel Discussion: Aligning Academia and Industry

Michael John, Erwin Kooi, Jos Weyers.