22nd ACM Conference on Computer and Communications Security

October 12 – 16, 2015

Denver, Colorado

Program

CCS 2015 and Co-located Workshops

Pre-conference Workshops
October 12, 2015

Please check monitors for last minute changes to room assignments

5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM 2015)	
6:45 – 8:00	Breakfast and Registration (Colorado Foyer and Central Registration Area)
8:00 – 9:00	Opening Remarks & Logistics – SPSM 2015 Meets in Colorado C
9:00 – 9:10	Welcome: David Lee (University of Toronto) & Glenn Wurster (BlackBerry)
9:10 – 10:20	**Keynote**: The Past, Present and Future of Digital Privacy. Alex Manea (BlackBerry)
10:45 – 11:00	Coffee Break (Colorado Foyer)
11:00 – 12:30	**Technical Session: Application Isolation; Session Chair: Alastair Beresford**
	Android Rooting: Methods, Detection, and Evasion *San-Tsai Sun (University of British Columbia), Andrea Cuadros (University of British Columbia), Konstantin Beznosov (University of British Columbia)*
	PrivacyGuard: A VPN-based Platform to Detect Information Leakage on Android Devices *Yihang Song (University of Waterloo), Urs Hengartner (University of Waterloo)*
	NJAS: sandboxing unmodified applications in non-rooted devices running stock Android *Antonio Bianchi (University of California, Santa Barbara), Yanick Fratantonio (University of California, Santa Barbara), Christopher Kruegel (University of California, Santa Barbara), Giovanni Vigna (University of California, Santa Barbara)*
12:30 – 2:00	Lunch
2:00 – 3:30	**Technical Session: Privacy; Session Chair TBD**
	AutoPPG: Automated Generation of Privacy Policy for Android Applications *Le Yu (The Hong Kong Polytechnic University), Tao Zhang (The Hong Kong Polytechnic University), Xiapu Luo (The Hong Kong Polytechnic University), Lei Xue (The Hong Kong Polytechnic University)*
	Supporting Privacy-Conscious App Update Decisions with User Reviews *Yuan Tian (Carnegie Mellon University), Bin Liu (Carnegie Mellon University), Weisi Dai (Google), Blase Ur (Carnegie Mellon University), Patrick Tague (Carnegie Mellon University), Lorrie Faith Cranor (Carnegie Mellon University)*
	The Impact of Timing on the Salience of Smartphone App Privacy Notices *Rebecca Balebako (Carnegie Mellon University), Florian Schaub (Carnegie Mellon University), Idris Adjerid (Notre Dame University), Alessandro Acquisti (Carnegie Mellon University), Lorrie Cranor (Carnegie Mellon University)*
3:40 – 4:00	Coffee Break (Colorado Foyer)
4:00 – 5:30	**Technical Session: Android Framework; Session Chair TBD**
	(Short Paper) Context-Specific Access Control: Conforming Permissions With User Expectations *Amir Rahmati (University of Michigan), Harsha V. Madhyastha (University of Michigan)*
	(Short Paper) Understanding the Service Life Cycle of Android Apps: An Exploratory Study *Kobra Khanmohammadi (Concordia University), Mohammad Reza Rejali (Concordia University), Abdelwahab Hamou-Lhadj (Concordia University)*
	Security Metrics for the Android Ecosystem *Daniel Thomas (University of Cambridge), Alastair Beresford (University of Cambridge), Andrew Rice (University of Cambridge)*
End of Workshop on Security and Privacy in Smartphones and Mobile Devices	

Workshop on Privacy in the Electronic Society (WPES 2015)	
6:45 – 8:00	Breakfast and Registration (Colorado Foyer and Central Registration Area)
8:00 – 8:20	Opening Remarks & Logistics – WPES 2015 meets in Colorado AB
9:15 – 10:45	**Technical Session – Web and Social Network Privacy; Session Chair: Aylin Caliskan-Islam**
	On the Privacy Practices of Just Plain Sites *Alyssa Phung Au (University of Pittsburgh School of Law); Amirhossein Aleyasen (University of Illinois Urbana); Oleksii Starov (Stony Brook University); Allan Schiffman (Commerce Net Palo Alto); Jeff Shrager (Commerce Net Palo Alto)*
	Known Unknowns: An Analysis of Twitter Censorship in Turkey *Rima S. Tanash (Rice University); Zhouhan Chen (Rice University); Tanmay Thakur (University of Houston); Dan S. Wallach (Rice University); Devika Subramanian (Rice University)*
	(Short Paper) - Inferring Unknown Privacy Control Policies in a Social Networking System *Amirreza Masoumzadeh (SUNY Albany)*
10:45 – 11:10	Coffee Break (Colorado Foyer)
11:10 – 12:30	**Technical Session – Mobile and Location Privacy; Session Chair: Reza Shokri**
	On the Unicity of Smartphone Applications *Jagdish Prasad Achara (Inria); Gergely Acs (Inria); Claude Castelluccia (Inria)*
	Strengthening Authentication with Privacy-Preserving Location Verification of Mobile Phones *Jan Camenisch (IBM Research - Zurich); Diego A. Ortiz-Yepes (IBM Research - Zurich); Franz-Stefan Preiss (IBM Research - Zurich)*
	(Short Paper) - The Same-Origin Attack against Location Privacy *George Theodorakopoulos (Cardiff University)*
12:30 – 2:00	Lunch
2:00 – 3:40	**Technical Session – Communication Privacy I; Session Chair: Aniket Kate**
	Notions of Deniable Message Authentication *Marc Fischlin (Technische Universität Darmstadt, Germany); Sogol Mazaheri (Technische Universität Darmstadt, Germany)*
	Sybil-resistant pseudonymization and pseudonym change without trusted third parties *Martin Florian (Karlsruhe Inst. of Tech.); Johannes Walter (Karlsruhe Inst. of Tech.); Ingmar Baumgart (Karlsruhe Inst. of Technology)*
	Rook: Using Video Games as a Low-Bandwidth Censorship Resistant Communication Platform *Paul Vines (University of Washington); Tadayoshi Kohno (University of Washington)*
3:40 – 4:00	Coffee Break (Colorado Foyer)
4:00 – 4:45	**Technical Session – Communication Privacy II; Session Chair: Aaron Johnson**
	Privately (and unlinkably) exchanging messages using a public bulletin board *Jaap-Henk Hoepman (Radboud University)*
	(Short Paper) ~ Towards Measuring Resilience in Anonymous Communication Networks *Fatemeh Shirazi (KU Leuven, iMinds); Claudia Diaz (KU Leuven, iMinds); Joss Wright (Oxford Internet Institute Univ. of Oxford)*
5:00 – 6:15	**Technical Session – Privacy Preserving Data Analysis**
	A High-Throughput Method to Detect Privacy-Sensitive Human Genomic Data *Vinicius V. Cogo (University of Lisbon); Alysson Bessani (University of Lisbon); Francisco M. Couto (University of Lisbon); Paulo Verissimo (University of Luxembourg)*
	Privacy-preserving User Matching *Paolo Gasti (New York Institute of Technology); Kasper Rasmussen (University of Oxford)*
	UnLinked: Private Proximity-based Off-line OSN Interaction *Sky Faber (University of California: Irvine); Ronald Petrlic (Commissioner for Data Protection Baden-Württemberg); Gene Tsudik (University of California: Irvine)*
End of Workshop on Privacy in the Electronic Society	

Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig 2015)	
6:45 – 8:00	Breakfast and Registration (Colorado Foyer and Central Registration Area)
8:00 – 8:20	Opening Remarks & Logistics – SafeConfig 2015 meets in Colorado D
8:30 – 10:45	**Keynote Speech: Integrated Adaptive Cyber Defense: Integration Spiral Results** Wende Peters, Johns Hopkins University Applied Physics Laboratory
10:45 – 11:10	Coffee Break (Colorado Foyer)
11:10 – 12:30	**Technical Session – Resiliency Analytics for Cyber Defense; Session Chair: Quanyan Zhu**
	Action Recommendation for Cyber Resilience *Sutanay Choudhury (PNNL, USA); Pin-Yu Chen (University of Michigan, USA); Indrajit Ray (Colorado State University, USA); Darren Curtis (PNNL, USA); Kiri Oler (PNNL, USA); Peter Nordquist (PNNL, USA); Luke Rodriguez (PNNL, USA)*
	Cyber Resilience-by-Construction: Modeling, Measuring & Verifying *Yasir Imtiaz Khan (UNC Charlotte, USA); Ehab Al-Shaer (UNC Charlotte, USA); Usman Rauf (UNC Charlotte, USA)*
	Estimating Risk Boundaries for Persistent and Stealthy Cyber-Attacks *Malik Awan (Cardiff University, UK); Peter Burnap (Cardiff University, UK); Omer Rana (Cardiff University, UK)*
	Who Touched My Mission: Towards Probabilistic Mission Impact Assessment *Xiaoyan Sun (Pennsylvania State University, USA); Anoop Singhal (NIST, USA); Peng Liu (Pennsylvania State University, USA)*
12:30 – 2:00	Lunch
2:00 – 3:40	**Technical Session – Decision Making for Secure System; Session Chair: Erin Fulp**
	Using Probability Densities to Evolve more Secure Software Configurations *Caroline Odell and Matthew McNiece (Wake Forest University, USA); Sarah Gage (Indiana University, USA); Howard Gage and Errin Fulp (Wake Forest University, USA)*
	Policy Specialization to Support Domain Isolation *Simone Mutti, Enrico Bacis (University of Bergamo, Italy); Stefano Paraboschi (University of Bergamo, Italy)*
	FlowMon: Detecting Malicious Switches in Software-Defined Networks *Andrzej Kamisiński (AGH University of Science and Technology, Poland); Carol J Fung (Virginia Commonwealth University, USA)*
	A Security Enforcement Framework for Virtual Machine Migration Auction *Santosh Majhi (IIT Bhubaneswar, India); Padmalochan Bera (IIT Bhubaneswar, India)*
	Behavior-dependent Routing: Responding to Anomalies with Automated Low-cost Measures (Short Paper) *Christopher Oehmen (PNNL, USA); Thomas Carroll (PNNL, USA); Patrick Paulsen (PNNL, USA); Daniel Best (PNNL, USA); Christine Noonan (PNNL, USA); Seth Thompson (PNNL, USA); Jeff Jensen (PNNL, USA); Glenn Fink (PNNL, USA); Elena Peterson (PNNL, USA)*
3:40 – 4:00	Coffee Break (Colorado Foyer)
4:00 – 6:00	**Panel: Active Cyber Defense for Resilient Infrastructure: Current Challenges and Future Directions** **Panel Moderator:** Christopher Oehmen **Panelists:** Ehab Al-Shaer, Arlette Hart, and Phil Quade
5:45 – 6:00	**Closing Remarks**
End of Workshop on Automated Decision Making for Active Cyber Defense	

2nd Workshop on Information Sharing and Collaborative Security (WISCS 2015)	
6:45 – 8:00	Breakfast and Registration (Colorado Foyer and Central Registration Area)
8:00 – 8:20	Opening Remarks & Logistics – WISCS 2015 meets in Gold Coin
8:20 – 9:25	**Keynote Speech**: Real World Information Exchange: Challenges and Insights, Freddy Dezeure, Head of CERT EU Session Chair: Thomas Sander
9:25 – 10:45	**Technical Session – Automated Intelligence Creation and Blacklists; Session Chair: Florian Kerschbaum**
	Data Mining for Efficient Collaborative Information Discovery *Samuel Perl, Bronwyn Woods, Brian Lindauer*
	Blacklist Ecosystem Analysis *Leigh Metcalf, Jonathan Spring*
10:45 – 11:10	Coffee Break (Colorado Foyer)
11:10 – 12:30	**Technical Session – Information Sharing Case Studies; Session Chair: Sarah Brown**
	ACTRA - A Case Study for Threat Information Sharing *Jon Haass, Gail-Joon Ahn, Frank Grimmelmann*
	Anonymity vs. Trust in Cyber-Security Collaboration *Stuart Murdoch, Nick Leaver*
12:30 – 2:00	Lunch
2:00 – 3:40	**Technical Session – Foundations and Economic Models for Information Sharing; Session Chair: Jose Such**
	Mandatory Security Information Sharing with Authorities: Implications on Investments in Internal Controls *Stefan Laube, Rainer Böhme*
	From Cyber Security Information Sharing to Threat Management *Sarah Brown, Joep Gommers, Oscar Serrano*
3:40 – 4:00	Coffee Break (Colorado Foyer)
4:00 – 5:20	**Technical Session – HCI and Actioning of Shared Data; Session Chair: Carol Fung**
	UX Aspects of Threat Information Sharing Platforms *Tomas Sander, Joshua Hailpern*
	An Actionable Threat Intelligence System Using a Publish-Subscribe Communications Model *Jyoti Verma, Nancy Cam-Winget, Syam Appala, David McGrew*
End of Workshop on Information Sharing and Collaborative Security	

Workshop on Moving Target Defense (MTD 2015)	
6:45 – 8:00	Breakfast and Registration (Colorado Foyer and Central Registration Area)
8:00 – 8:15	Opening Remarks & Logistics – MTD 2015 meets in Colorado G
8:15 – 9:15	**Keynote Speech**: From Fine Grained Code Diversity to Execute-Only-Memory: The Cat and Mouse Game Between Attackers and Defenders Continues, Michael Franz (University of Californian, Irvine)
9:15 – 10:45	**Technical Session: MTD Modeling and Evaluation 1; Session Chair: Chris Lamb**
	A Quantitative Framework for Moving Target Defense Effectiveness Evaluation *Kara Zaffarano (Siege Technologies); Joshua Taylor (Siege Technologies); Samuel Hamilton (Siege Technologies)*
	A Theory of Cyber Attacks -- A Step Towards Analyzing MTD Systems *Rui Zhuang (Kansas State University); Alexandru G. Bardas (Kansas State University); Scott A. Deloach (Kansas State University); Xinming Ou (Kansas State University)*
	Probabilistic Performance Analysis of Moving Target and Deception Reconnaissance *Michael Crouse (Harvard University); Bryan Prosser (Wake Forest University); Errin Fulp (Wake Forest University)*
10:45 – 11:10	Coffee Break (Colorado Foyer)
11:10 – 12:30	**Technical Session: MTD Technologies 1; Session Chair: Xinming Ou**
	Characterizing Network-Based Moving Target Defenses *Marc Green (Worcester Polytechnic Institute); Douglas MacFarland (Worcester Polytechnic Institute); Doran Smestad (Worcester Polytechnic Institute); Craig Shue (Worcester Polytechnic Institute)*
	The SDN Shuffle: Creating a Moving-Target Defense using Host-based Software-Defined Networking *Douglas MacFarland (Worcester Polytechnic Institute); Craig Shue (Worcester Polytechnic Institute)*
	VINE: A Cyber Emulation Environment for MTD Experimentation *Thomas C Eskridge (Florida Institute of Technology); Marco Carvalho (Florida Institute of Technology); Evan Stoner (Florida Institute of Technology); Troy Toggweiler (Florida Institute of Technology); Adrian Granados (Florida Institute of Technology)*
	Adaptive Just-In-Time Code Diversification *Abhinav Jangda (IIT (BHU) Varanasi); Mohit Mishra (IIT (BHU) Varanasi); Bjorn De Sutter (Ghent University)*
12:30 – 1:45	Lunch
1:45 – 2:45	**Keynote Speech**: Getting Beyond Tit for Tat: Better Strategies for Moving Target Prototyping and Evaluation Hamid Okhravi, (MIT Lincoln Laboratory)
2:45 – 3:45	**Technical Session: MTD Modeling and Evaluation 2; Session Chair: Zhuo Lu**
	Empirical Game-Theoretic Analysis for Moving Target Defense *Achintya Prakash (University of Michigan); Michael Wellman (University of Michigan)*
	Optimal Defense Policies for Partially Observable Spreading Processes on Bayesian Attack Graph *Erik Miehling (University of Michigan); Mohammad Rasouli (University of Michigan); Demosthenis Teneketzis (University of Michigan)*
3:45 – 4:00	Coffee Break (Colorado Foyer)
4:00 – 5:30	**Technical Session: MTD Technologies 2; Session Chair: Thomas Eskridge**
	DHT Blind Rendezvous for Session Establishment in Network Layer Moving Target Defenses *Christopher Morrell (Virginia Tech); Reese Moore (Virginia Tech); Randy Marchany (Virginia Tech); Joseph Tront (Virginia Tech)*
	To Be Proactive or Not: A Framework to Model Cyber Maneuvers for Critical Path Protection in MANETs *Zhuo Lu (University of Memphis); Lisa Marvel (Army Research Laboratory); Cliff Wang (North Carolina State University)*
	Software Protection with Code Mobility Alessandro Cabutto (University of East London); Paolo Falcarin (University of East London); Bert Abrath (Ghent University); Bart Coppens (Ghent University); Bjorn De Sutter (Ghent University)
5:30 – 6:15	**Panel Discussion and Wrap Up**
End of Workshop on Moving Target Defense	

CCS 2015 Main Conference
October 13-15, 2015

CCS 2015 MAIN CONFERENCE, TUESDAY OCTOBER 13				
	TRACK A	**TRACK B**	**TRACK C**	**Tutorial**
	Room: Denver 1 – 3	**Room: Colorado E**	**Room: Colorado A – D**	**Room: Gold Coin**
6:45 – 8:00	Breakfast and Registration (Colorado Foyer & Central Registration Area)			
8:00 – 8:20	Opening Remarks (Colorado A – E)			
8:30 – 9:30	Keynote Speech – Dr. Edward Felten (Colorado A – E); Session Chair: Indrajit Ray			
9:30 – 9:50	Short Break for Room Setup			
	Session 1A **How Real World Crypto Fails** Session Chair - Ahmad-Reza Sadeghi (TU Darmstadt)	Session 1B **iOS and MAC OS Security** Session Chair - Kapil Singh (IBM Research)	Session 1C **Censorship and Resistance** Session Chair - Hamed Okhravi (MIT Lincoln Labs)	Fraud Detection through Graph-Based User Behavior Modeling — *Alex Beutel (Carnegie Melon University); Leman Akoglu (Stony Brook University); Christos Faloutsos (Carnegie Melon University)*
9:55 – 10:20	Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice *David Adrian (Univ. of Michigan); Karthikeyan Bhargavan (INRIA Paris-Rocquencourt); Zakir Durumeric (Univ. of Michigan); Pierrick Gaudry (INRIA Nancy-Grand Est, CNRS and Université de Lorraine); Matthew Green (Johns Hopkins Univ.); J. Alex Halderman (Univ. of Michigan); Nadia Heninger (Univ. of Pennsylvania); Drew Springall (Univ. of Michigan); Emmanuel Thomé (INRIA Nancy-Grand Est, CNRS and Université de Lorraine); Luke Valenta (Univ. of Pennsylvania); Benjamin VanderSloot (Univ. of Michigan); Eric Wustrow (Univ. of Michigan); Santiago Zanella-Béguelin (Microsoft Research); Paul Zimmermann (INRIA Nancy-Grand Est, CNRS and Université de Lorraine)*	Cracking App Isolation on Apple: Unauthorized Cross-App Resource Access on MAC OS X and iOS *Luyi Xing (Indiana Univ. Bloomington); Xiaolong Bai (Indiana Univ. Bloomington & Tsinghua Univ.); Tongxin Li (Peking Univ.); XiaoFeng Wang (Indiana Univ. Bloomington); Kai Chen (Indiana Univ. Bloomington & Chinese Academy of Sciences); Xiaojing Liao (Georgia Institute of Technology); Shi-Min Hu (Tsinghua Univ.); Xinhui Han (Peking Univ.)*	Seeing through Network Protocol Obfuscation *Liang Wang (Univ. of Wisconsin); Kevin P. Dyer (Portland State Univ.); Aditya Akella (Univ. of Wisconsin); Thomas Ristenpart (Univ. of Wisconsin); Thomas Shrimpton (Portland State Univ.)*	

	TRACK A	TRACK B	TRACK C	Tutorial
	Room: Denver 1 – 3	Room: Colorado E	Room: Colorado A – D	Room: Gold Coin
	Session 1A **How Real World Crypto Fails**	Session 1B **iOS and MAC OS Security**	Session 1C **Censorship and Resistance**	Fraud Detection through Graph-Based User Behavior Modeling — *Alex Beutel (Carnegie Melon University); Leman Akoglu (Stony Brook University); Christos Faloutsos (Carnegie Melon University)*
	Session Chair - Ahmad-Reza Sadeghi (TU Darmstadt)	Session Chair - Kapil Singh (IBM Research)	Session Chair - Hamed Okhravi (MIT Lincoln Labs)	
10:20 – 10:45	Ciphertext-only Cryptanalysis on Hardened Mifare Classic Cards *Carlo Meijer (Radboud University); Roel Verdult (Radboud University)*	iRiS: Vetting Private API Abuse in iOS Applications *Zhui Deng (Purdue Univ.); Brendan Saltaformaggio (Purdue Univ.); Xiangyu Zhang (Purdue Univ.); Dongyan Xu (Purdue Univ.)*	CacheBrowser: Bypassing Chinese Censorship without Proxies Using Cached Content *John A. Holowczak (Univ. of Massachusetts Amherst); Amir Houmansadr (Univ. of Massachusetts Amherst)*	
10:45 – 11:10	Coffee Break (Colorado Foyer)			
	Session 2A **Authenticated Encryption**	Session 2B **Android & Web Forensics**	Session 2C **Password Security**	Fraud Detection through Graph-Based User Behavior Modeling — *Alex Beutel (Carnegie Melon University); Leman Akoglu (Stony Brook University); Christos Faloutsos (Carnegie Melon University)*
	Session Chair - Moti Yung (Google Inc. & Columbia Univ.)	Session Chair - Danfeng Yao (Virginia Tech.)	Session Chair – Joseph Bonneau (Stanford Univ. & EFF)	
11:10 – 11:35	Automated Analysis and Synthesis of Authenticated Encryption Schemes *Viet Tung Hoang (Univ. of Maryland, Georgetown Univ.); Jonathan Katz (Univ. of Maryland); Alex J. Malozemoff (Univ. of Maryland)*	GUITAR: Piecing Together Android App GUIs from Memory Images *Brendan Saltaformaggio (Purdue Univ.); Rohit Bhatia (Purdue Univ.); Zhongshu Gu (Purdue Univ.); Xiangyu Zhang (Purdue Univ.); Dongyan Xu (Purdue Univ.)*	Monte Carlo Strength Evaluation: Fast and Reliable Password Checking *Matteo Dell'Amico (Symantec Research Labs); Maurizio Filippone (Univ. of Glasgow)*	
11:35 – 12:00	Leakage-Resilient Authentication and Encryption from Symmetric Cryptographic Primitives *Olivier Pereira (Universite catholique de Louvain); Francois-Xavier Standaert (Universite catholique de Louvain); Srinivas Vivek (Univ. of Luxembourg & Univ. of Bristol)*	WebCapsule: Towards a Lightweight Forensic Engine for Web Browsers *Christopher Neasbitt (Univ. of Georgia); Bo Li (Univ. of Georgia); Roberto Perdisci (Univ. of Georgia); Long Lu (Stony Brook Univ.); Kapil Singh (IBM Research); Kang Li (Univ. of Georgia)*	Surpass: System-initiated user-replaceable passwords *Jun Ho Huh (Honeywell ACS Labs); Seongyeol Oh (Sungkyunkwan Univ.); Hyoungshick Kim (Sungkyunkwan Univ.); Konstantin Beznosov (Univ. of British Columbia); Apurva Mohan (Honeywell ACS Labs); Raj Rajagopalan (Honeywell ACS Labs)*	

	TRACK A	TRACK B	TRACK C	Tutorial
	Room: Denver 1 – 3	**Room: Colorado E**	**Room: Colorado A – D**	**Room: Gold Coin**
	Session 2A **Authenticated Encryption**	Session 2B **Android & Web Forensics**	Session 2C **Password Security**	
	Session Chair - Moti Yung (Google Inc. & Columbia Univ.)	Session Chair - Danfeng Yao (Virginia Tech.)	Session Chair – Joseph Bonneau (Stanford Univ. & EFF)	
12:00 – 12:25	GCM-SIV: Full Nonce Misuse-Resistant Authenticated Encryption at Under One Cycle per Byte *Shay Gueron (Univ. of Haifa); Yehuda Lindell (Bar-Ilan Univ.)*	VCR: App-Agnostic Recovery of Photographic Evidence from Android Device Memory Images *Brendan Saltaformaggio (Purdue Univ.); Rohit Bhatia (Purdue Univ.); Zhongshu Gu (Purdue Univ.); Xiangyu Zhang (Purdue Univ.); Dongyan Xu (Purdue Univ.)*	Optimal Distributed Password Verification *Jan Camenisch (IBM Research - Zurich); Anja Lehmann (IBM Research - Zurich); Gregory Neven (IBM Research - Zurich)*	
12:30 – 2:00	**Lunch (Colorado F – J)**			
	Session 3A Using Cryptocurrency	Session 3B Memory Randomization	Session 3C Wireless and VoLTE Security	
	Session Chair - Taesoo Kim (Georgia Inst. of Tech.)	Session Chair - Long Lu (Stony Brook Univ.)	Session Chair - Yao Liu (Univ. of South Florida)	
2:00 – 2:25	How to Use Bitcoin to Play Decentralized Poker *Ranjit Kumaresan (MIT); Tal Moran (IDC Herzliya); Iddo Bentov (Technion)*	It's a TRAP: Table Randomization and Protection against Function Reuse Attacks *Stephen Crane (Univ. of California, Irvine); Stijn Volckaert (Universiteit Gent); Felix Schuster (Ruhr-Universität Bochum); Christopher Liebchen (Technische Universität Darmstadt); Per Larsen (Univ. of California, Irvine); Lucas Davi (Technische Universität Darmstadt); Ahmad-Reza Sadeghi (Technische Universität Darmstadt); Thorsten Holz (Ruhr-Universität Bochum); Bjorn De Sutter (Universiteit Gent); Michael Franz (Univ. of California, Irvine)*	Location-restricted Service Access Control Leveraging Pinpoint Waveforming *Tao Wang (Univ. of South Florida); Yao Liu (Univ. of South Florida); Qingqi Pei (Xidian Univ.); Tao Hou (Univ. of South Florida)*	

	TRACK A	TRACK B	TRACK C	Tutorial
	Room: Denver 1 – 3	Room: Colorado E	Room: Colorado A – D	Room: Gold Coin
	Session 3A Using Cryptocurrency	Session 3B Memory Randomization	Session 3C Wireless and VoLTE Security	
	Session Chair - Taesoo Kim (Georgia Inst. of Tech.)	Session Chair - Long Lu (Stony Brook Univ.)	Session Chair - Yao Liu (Univ. of South Florida)	
2:25 – 2:50	Micropayments for Decentralized Currencies *Rafael Pass (Cornell Tech); Abhi Shelat (U Virginia)*	Heisenbyte: Thwarting Memory Disclosure Attacks using Destructive Code Reads *Adrian Tang (Columbia Univ.); Simha Sethumadhavan (Columbia Univ.); Salvatore Stolfo (Columbia Univ.)*	SafeDSA: Safeguard Dynamic Spectrum Access against Fake Secondary Users *Xiaocong Jin (Arizona State Univ.); Jingchao Sun (Arizona State Univ.); Rui Zhang (Univ. of Hawaii); Yanchao Zhang (Arizona State Univ.)*	
2:50 – 3:15	Liar, Liar, Coins on Fire! --- Penalizing Equivocation By Loss of Bitcoins *Tim Ruffing (CISPA, Saarland Univ.); Aniket Kate (CISPA, Saarland Univ.); Dominique Schröder (CISPA, Saarland Univ.)*	Timely Rerandomization for Mitigating Memory Disclosures *David Bigelow (MIT Lincoln Laboratory); Thomas Hobson (MIT Lincoln Laboratory); Robert Rudd (MIT Lincoln Laboratory); William Streilein (MIT Lincoln Laboratory); Hamed Okhravi (MIT Lincoln Laboratory)*	Insecurity of Voice Solution VoLTE in LTE Mobile Networks *Chi-Yu Li (UCLA); Guan-Hua Tu (UCLA); Chunyi Peng (OSU); Zengwen Yuan (UCLA); Yuanjie Li (UCLA); Songwu Lu (UCLA); Xinbing Wang (Shanghai Jiao Tong Univ.)*	
3:15 – 3:40	Traitor Deterring Schemes: Using Bitcoin as Collateral for Digital Content *Aggelos Kiayias (National and Kapodistrian Univ. of Athens); Qiang Tang (Univ. of Connecticut);*	ASLR-Guard: Stopping Address Space Leakage for Code Reuse Attacks *Kangjie Lu (Georgia Institute of Technology); Chengyu Song (Georgia Institute of Technology); Byoungyoung Lee (Georgia Institute of Technology); Simon P. Chung (Georgia Institute of Technology); Taesoo Kim (Georgia Institute of Technology); Wenke Lee (Georgia Institute of Technology)*	Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations *Hongil Kim (KAIST); Dongkwan Kim (KAIST); Minhee Kwon (KAIST); HyungSeok Han (KAIST); Yeongjin Jang (Georgia Institute of Technology); Dongsu Han (KAIST); Taesoo Kim (Georgia Institute of Technology); Yongdae Kim (KAIST)*	
3:40 – 4:00	Coffee Break (Colorado Foyer)			

	TRACK A	TRACK B	TRACK C	Tutorial
	Room: Denver 1 – 3	Room: Colorado E	Room: Colorado A – D	Room: Gold Coin
	Session 4A Applied Cryptography	Session 4B Software Vulnerabilities	Session 4C Assessing Current Defenses	
	Session Chair - Dario Fiore (IMDEA Software Inst.)	Session Chair – Mathias Payer (Purdue University)	Session Chair - Roberto Perdisci (Univ. of Georgia)	
4:00 – 4:25	Defeating IMSI Catchers *Fabian van den Broek (Radboud Univ. Nijmegen); Roel Verdult (Radboud Univ. Nijmegen); Joeri de Ruiter (Univ. of Birmingham)*	Static Detection of Packet Injection Vulnerabilities -- A Case for Identifying Attacker-controlled Implicit Information Leaks *Qi Alfred Chen (Univ. of Michigan); Zhiyun Qian (Univ. of California Riverside); Yunhan Jack Jia (Univ. of Michigan); Yuru Shao (Univ. of Michigan); Z. Morley Mao (Univ. of Michigan)*	UCognito: Private Browsing without Tears *Meng Xu (Georgia Institute of Technology); Yeongjin Jang (Georgia Institute of Technology); Xinyu Xing (Georgia Institute of Technology); Taesoo Kim (Georgia Institute of Technology); Wenke Lee (Georgia Institute of Technology)*	
4:25 – 4:50	DEMOS-2: Scalable E2E Verifiable Elections without Random Oracles *Aggelos Kiayias (National and Kapodistrian Univ. of Athens); Thomas Zacharias (National and Kapodistrian Univ. of Athens); Bingsheng Zhang (Lancaster Univ.)*	Unearthing Stealthy Program Attacks Buried in Extremely Long Execution Paths *Xiaokui Shu (Virginia Tech); Danfeng (Daphne) Yao (Virginia Tech); Naren Ramakrishnan (Virginia Tech)*	Security by Any Other Name: On the Effectiveness of Provider Based Email Security *Ian Foster (Univ. of California, San Diego); Jon Larson (Univ. of California, San Diego); Max Masich (Univ. of California, San Diego); Alex C. Snoeren (Univ. of California, San Diego); Stefan Savage (Univ. of California, San Diego); Kirill Levchenko (Univ. of California, San Diego)*	
4:50 – 5:15	Subversion-Resilient Signature Schemes *Giuseppe Ateniese (Sapienza Univ. of Rome); Bernardo Magri (Sapienza Univ. of Rome); Daniele Venturi (Sapienza Univ. of Rome)*	From Collision To Exploitation: Unleashing Use-After-Free Vulnerabilities in Linux Kernel *Wen Xu (Shanghai Jiao Tong Univ.); Juanru Li (Shanghai Jiao Tong Univ.); Junliang Shu (Shanghai Jiao Tong Univ.); Wenbo Yang (Shanghai Jiao Tong Univ.); Tianyi Xie (Shanghai Jiao Tong Univ.); Yuanyuan Zhang (Shanghai Jiao Tong Univ.); Dawu Gu (Shanghai Jiao Tong Univ.)*	Certified PUP: Abuse in Authenticode Code Signing *Platon Kotzias (IMDEA Software Institute); Srdjan Matic (Universita degli Studi di Milano); Richard Rivera (IMDEA Software Institute); Juan Caballero (IMDEA Software Institute)*	

	TRACK A	TRACK B	TRACK C	Tutorial
	Room: Denver 1 – 3	Room: Colorado E	Room: Colorado A – D	Room: Gold Coin
	Session 4A Applied Cryptography	Session 4B Software Vulnerabilities	Session 4C Assessing Current Defenses	
	Session Chair - Dario Fiore (IMDEA Software Inst.)	Session Chair - Ben Livshits (Microsoft Research)	Session Chair - Roberto Perdisci (Univ. of Georgia)	
5:15 – 5:40	Walls Have Ears! Opportunistically Communicating Secret Messages Over the Wiretap Channel: from Theory to Practice *Qian Wang (Wuhan Univ.); Kui Ren (The State Univ. of New York at Buffalo); Guancheng Li (Wuhan Univ.); Chenbo Xia (Wuhan Univ.); Xiaobing Chen (Wuhan Univ.); Zhibo Wang (Wuhan Univ.); Qin Zou (Wuhan Univ.)*	VCCFinder: Finding Potential Vulnerabilities in Open-Source Projects to Assist Code Audits *Henning Perl (Fraunhofer FKIE); Daniel Arp (Universität Göttingen); Sergej Dechand (Universität Bonn); Fabian Yamaguchi (Universität Göttingen); Sascha Fahl (Saarland University); Yasemin Acar (Saarland University); Konrad Rieck (Universität Göttingen); Matthew Smith (Universität Bonn)*	A Multi-Modal Neuro-Physiological Study of Phishing Detection and Malware Warnings *Ajaya Neupane (Univ. of Alabama at Birmingham); Md. Lutfor Rahman (Marvin Technologies); Nitesh Saxena (Univ. of Alabama at Birmingham); Leanne Hirshfield (Syracuse Univ.)*	
5:45 – 6:45		CCS Business Meeting		
7:00 – 9:00	Poster Session; Conference Reception and Cocktail (Colorado F – J)			

CCS 2015 MAIN CONFERENCE, WEDNESDAY OCTOBER 14				
	TRACK A	**TRACK B**	**TRACK C**	**TUTORIAL**
	Room: Denver 1 – 3	**Room: Colorado E**	**Room: Colorado A – D**	**Room: Gold Coin**
6:45 – 8:00	Breakfast and Registration (Colorado Foyer and Central Registration Area)			
8:30 – 9:30	Keynote Speech – Dr. Moti Yung (Colorado A – E); Session Chair: Trent Jaeger			
9:30 – 9:50	Short Break			
	Session 5A Computing on Encrypted Data	Session 5B Understanding Android Apps	Session 5C Scanning the Web	
	Session Chair – Florian Kerschbaum (SAP)	Session Chair – Gang Tan (Lehigh Univ.)	Session Chair – Amir Houmansadr (Univ. of Mass.)	
9:55 – 10:20	Efficient Genome-Wide, Privacy-Preserving Similar Patient Query based on Private Edit Distance *Xiao Shaun Wang (Univ. of Maryland); Yan Huang (Indiana Univ. Bloomington); Yongan Zhao (Indiana Univ. Bloomington); Haixu Tang (Indiana Univ. Bloomington); Xiaofeng Wang (Indiana Univ. Bloomington); Diyue Bu (Indiana Univ. Bloomington)*	Towards Automatic Generation of Security-Centric Descriptions for Android Apps *Mu Zhang (NEC Laboratories America); Yue Duan (Syracuse Univ.); Qian Feng (Syracuse Univ.); Heng Yin (Syracuse Univ.)*	A Search Engine Backed by Internet-Wide Scanning *Zakir Durumeric (Univ. of Michigan); David Adrian (Univ. of Michigan); Ariana Mirian (Univ. of Michigan); Michael Bailey (Univ. of Illinois at Urbana-Champaign); J. Alex Halderman (Univ. of Michigan)*	Program Analysis for Mobile Application Integrity — *Marco Pistoia (IBM T. J. Watson Research Center)*
10:20 – 10:45	GRECS: Graph Encryption for Approximate Shortest Distance Queries *Xianrui Meng (Boston Univ.); Seny Kamara (Microsoft Research); Kobbi Nissim (Ben-Gurion Univ.); George Kollios (Boston Univ.)*	AUTOREB: Automatically Understanding the Review-to-Behavior Fidelity in Android Applications *Deguang Kong (Samsung Research America); Lei Cen (Purdue Univ.); Hongxia Jin (Samsung Research America)*	Sunlight: Fine-grained Targeting Detection at Scale with Statistical Confidence *Mathias Lecuyer (Columbia Univ.); Riley Spahn (Columbia Univ.); Yannis Spiliopoulos (Columbia Univ.); Augustin Chaintreau (Columbia Univ.); Roxana Geambasu (Columbia Univ.); Daniel Hsu (Columbia Univ.)*	
10:45 – 11:05	Coffee Break (Colorado Foyer)			

	TRACK A	TRACK B	TRACK C	TUTORIAL
	Room: Denver 1 – 3	Room: Colorado E	Room: Colorado A – D	Room: Gold Coin
	Session 6A Garbled Circuits	Session 6B Web Application Security	Session 6C Property Preserving Encryption	
	Session Chair - Yan Huan (Indiana Univ. Bloomington)	Session Chair - Adam Doupé (Arizona State Univ.)	Session Chair - Yinqian Zhang (Ohio State Univ.)	
11:10 – 11:35	Fast Garbling of Circuits Under Standard Assumptions *Shay Gueron (Univ. of Haifa and Intel); Yehuda Lindell (Bar Ilan Univ.); Ariel Nof (Bar Ilan Univ.); Benny Pinkas (Bar Ilan Univ.)*	FlowWatcher: Defending against Data Disclosure Vulnerabilities in Web Applications *Divya Muthukumaran (Imperial College London); Dan O'Keeffe (Imperial College London); Christian Priebe (Imperial College London); David Eyers (Univ. of Otago); Brian Shand (NCRS, Public Health England); Peter Pietzuch (Imperial College London)*	Inference Attacks on Property-Preserving Encrypted Databases *Muhammad Naveed (Univ. of Illinois at Urbana-Champaign); Seny Kamara (Microsoft Research); Charles V Wright (Portland State Univ.)*	Program Analysis for Mobile Application Integrity — *Marco Pistoia (IBM T. J. Watson Research Center)*
11:35 – 12:00	Blazing Fast 2PC in the Offline/Online Setting with Security for Malicious Adversaries *Yehuda Lindell (Bar-Ilan Univ.); Ben Riva (Bar-Ilan Univ.)*	Detecting and Exploiting Second Order Denial-of-Service Vulnerabilities in Web Applications *Oswaldo Olivo (The Univ. of Texas at Austin); Isil Dillig (The Univ. of Texas at Austin); Calvin Lin (The Univ. of Texas at Austin)*	Frequency-Hiding Order-Preserving Encryption *Florian Kerschbaum (SAP)*	
12:00 – 12:25	Fast and Secure Three-party Computation: The Garbled Circuit Approach *Payman Mohassel (Yahoo Labs); Mike Rosulek (Oregon State Univ.); Ye Zhang (Penn State Univ.)*	Inlined Information Flow Monitoring for JavaScript *Andrey Chudnov (Stevens Institute of Technology); David A. Naumann (Stevens Institute of Technology)*	Leakage-Abuse Attacks Against Searchable Encryption *David Cash (Rutgers Univ.); Paul Grubbs (Cornell Univ., SkyHigh Networks); Jason Perry (Rutgers Univ.); Thomas Ristenpart (Univ. of Wisconsin)*	
12:30 – 2:00	Lunch (Colorado F – J)			

	TRACK A	TRACK B	TRACK C	TUTORIAL
	Room: Denver 1 – 3	Room: Colorado E	Room: Colorado A – D	Room: Gold Coin
	Session 7A CryptoCurrency	Session 7B Analyzing Obfuscated Code	Session 7C Online Social Networks	
	Session Chair – Abhi Shelat (Univ. of Virginia)	Session Chair – Juan Caballero (IMDEA Software Inst.)	Session Chair – Nick Nikiforakis (Stony Brook Univ.)	
2:00 – 2:25	Nonoutsourceable Scratch-Off Puzzles to Discourage Bitcoin Mining Coalitions *Andrew Miller (Univ. of Maryland); Ahmed Kosba (Univ. of Maryland); Elaine Shi (Cornell Univ.); Jonathan Katz (Univ. of Maryland)*	Symbolic Execution of Obfuscated Code *Babak Yadegari (Univ. of Arizona); Saumya Debray (Univ. of Arizona)*	Face/Off: Preventing Privacy Leakage From Photos in Social Networks *Panagiotis Ilia (FORTH); Iasonas Polakis (Columbia Univ.); Elias Athanasopoulos (FORTH); Federico Maggi (Politecnico di Milano); Sotiris Ioannidis (FORTH)*	
2:25 – 2:50	Tampering with the Delivery of Blocks and Transactions in Bitcoin *Arthur Gervais (ETH Zurich); Hubert Ritzdorf (ETH Zurich); Ghassan O. Karame (NEC Laboratories Europe); Srdjan Capkun (ETH Zurich)*	CoDisasm : Medium scale concatic disassembly of self-modifying binaries with overlapping instructions *Guillaume Bonfante (Université de Lorraine); José Fernandez (Ecole Politechnique, Canada); Jean-Yves Marion (Université de Lorraine); Rouxel (Université de Lorraine); Sabatier (INRIA); Thierry (Université de Lorraine)*	CrowdTarget: Target-based Detection of Crowdturfing in Online Social Networks *Jonghyuk Song (Samsung Electronics); Sangho Lee (Pohang Univ. of Science and Technology); Jong Kim (Pohang Univ. of Science and Technology)*	
2:50 – 3:15	Demystifying Incentives In The Consensus Computer *Loi Luu (National Univ. of Singapore); Jason Teutsch (National Univ. of Singapore); Raghav Kulkarni (National Univ. of Singapore); Prateek Saxena (National Univ. of Singapore)*	LOOP: Logic-Oriented Opaque Predicate Detection in Obfuscated Binary Code *Jiang Ming (The Pennsylvania State Univ.); Dongpeng Xu (The Pennsylvania State Univ.); Li Wang (The Pennsylvania State Univ.); Dinghao Wu (The Pennsylvania State Univ.)*	Exploiting Temporal Dynamics in Sybil Defenses *Peng Gao (Princeton Univ.); Changchang Liu (Princeton Univ.); Matthew Wright (Univ. of Texas at Arlington); Prateek Mittal (Princeton Univ.)*	
3:15 – 3:40	Provisions: Privacy-preserving proofs of solvency for Bitcoin exchanges *Jeremy Clark (Concordia Univ.); Gaby Dagher (Concordia Univ.); Benedikt Bünz (Stanford Univ.); Joseph Bonneau (Stanford Univ. & EFF); Dan Boneh (Stanford Univ.)*	MalGene: Automatic Extraction of Malware Analysis Evasion Signature *Dhilung Kirat (UC Santa Barbara); Giovanni Vigna (UC Santa Barbara)*	Where's Wally? Precise User Discovery Attacks in Location Proximity Services *Iasonas Polakis (Columbia Univ.); George Argyros (Columbia Univ.); Theofilos Petsios (Columbia Univ.); Suphannee Sivakorn (Columbia Univ.); Angelos D. Keromytis (Columbia Univ.)*	
3:40 – 4:00	Coffee Break (Colorado Foyer)			

	TRACK A	TRACK B	TRACK C	TUTORIAL
	Room: Denver 1 – 3	Room: Colorado E	Room: Colorado A – D	Room: Gold Coin
	Session 8A Outsourced Storage	Session 8B Control Flow Integrity	Session 8C Enhancing Trust	
	Session Chair - Matteo Maffei (Saarland Univ.)	Session Chair - Xinming Ou (Univ. of South Florida)	Session Chair - Brent Kang (KAIST)	
4:00 – 4:25	Practicing Oblivious Access on Cloud Storage: the Gap, the Fallacy and the New Way Forward *Vincent Bindschaedler (Univ. of Illinois at Urbana-Champaign); Muhammad Naveed (Univ. of Illinois at Urbana-Champaign); Xiaorui Pan (Indiana Univ. Bloomington); XiaoFeng Wang (Indiana Univ. Bloomington); Yan Huang (Indiana Univ. Bloomington)*	Control Jujutsu: On the Weaknesses of Fine-Grained Control Flow Integrity *Isaac Evans (MIT Lincoln Laboratory); Fan Long (MIT CSAIL); Ulziibayar Otgonbaatar (MIT CSAIL); Howard Shrobe (MIT CSAIL); Martin Rinard (MIT CSAIL); Hamed Okhravi (MIT Lincoln Laboratory); Stelios Sidiroglou-Douskos (MIT CSAIL)*	SEDA: Scalable Embedded Device Attestation *N. Asokan (Aalto Univ. and Univ. of Helsinki); Ferdinand Brasser (Technische Universität Darmstadt); Ahmad Ibrahim (Technische Universität Darmstadt); Ahmad-Reza Sadeghi (Technische Universität Darmstadt); Matthias Schunter (Intel Collaborative Research Institute for Secure Computing (ICRI-SC), Darmstadt); Gene Tsudik (Univ. of California, Irvine); Christian Wachsmann (Technische Universität Darmstadt)*	
4:25 – 4:50	Circuit ORAM: On Tightness of the Goldreich-Ostrovsky Lower Bound *Xiao Shaun Wang (Univ. of Maryland); T-H. Hubert Chan (HKU); Elaine Shi (Cornell Univ.)*	Per-Input Control-Flow Integrity *Ben Niu (Lehigh Univ.); Gang Tan (Lehigh Univ.)*	TrustOTP: Transforming Smartphones into Secure One-Time Password Tokens *He Sun (College of William and Mary & Chinese Academy of Sciences); Kun Sun (College of William and Mary); Yuewu Wang (Chinese Academy of Sciences); Jiwu Jing (Chinese Academy of Sciences)*	

	TRACK A	TRACK B	TRACK C	TUTORIAL
	Room: Denver 1 – 3	Room: Colorado E	Room: Colorado A – D	Room: Gold Coin
	Session 8A Outsourced Storage	Session 8B Control Flow Integrity	Session 8C Enhancing Trust	
	Session Chair - Matteo Maffei (Saarland Univ.)	Session Chair - Xinming Ou (Univ. of South Florida)	Session Chair - Brent Kang (KAIST)	
4:50 – 5:15	Constant Communication ORAM with Small Blocksize *Tarik Moataz (Colorado State Univ. & Telecom Bretagne); Travis Mayberry (United States Naval Academy); Erik-Oliver Blass (Airbus Group Innovations)*	Practical Context-Sensitive CFI *Victor van der Veen (VU University Amsterdam); Dennis Andriesse (VU University Amsterdam); Enes Göktas (VU University Amsterdam); Ben Gras (VU University Amsterdam); Lionel Sambuc (VU University Amsterdam); Asia Slowinska (VU University Amsterdam, Lastline, Inc.); Herbert Bos (VU University Amsterdam); Cristiano Giuffrida (VU University Amsterdam);*	Trusted Display on Untrusted Commodity Platforms *Miao Yu (Carnegie Mellon Univ.); Virgil D. Gligor (Carnegie Mellon Univ.); Zongwei Zhou (Carnegie Mellon Univ.)*	
5:15 – 5:40	Secure Deduplication of Encrypted Data without Additional Independent Servers *Jian Liu (Aalto Univ.); N. Asokan (Aalto Univ. and Univ. of Helsinki); Benny Pinkas (Bar Ilan Univ.);*	CCFI: Cryptographically Enforced Control Flow Integrity *Ali Jose Mashtizadeh (Stanford Univ.); Andrea Bittau (Stanford Univ.); Dan Boneh (Stanford Univ.); David Mazieres (Stanford Univ.)*	PyCRA: Physical Challenge-Response Authentication for Active Sensors Under Spoofing Attacks *Yasser Shoukry (UCLA); Paul Martin (UCLA); Yair Yona (UCLA); Suhas Diggavi (UCLA); Mani Srivastava (UCLA)*	
5:40 – 6:05	Transparent Data Deduplication in the Cloud *Frederik Armknecht (Univ. of Mannheim); Jens-Matthias Bohli (NEC Laboratories Europe); Ghassan O. Karame (NEC Laboratories Europe); Franck Youssef (NEC Laboratories Europe)*	Losing Control: On the Effectiveness of Control-Flow Integrity under Stack Attacks *Christopher Liebchen, Marco Negro (Technische Universität Darmstadt); Per Larsen (Univ. of California, Irvine); Lucas Davi, Ahmad-Reza Sadeghi (Technische Universität Darmstadt); Stephen Crane (Univ. of California, Irvine); Mohaned Qunaibit (Univ. of California, Irvine); Michael Franz (Univ. of California, Irvine); Mauro Conti (Univ. of Padua)*	Clean Application Compartmentalization with SOAAP *Khilan Gudka (Univ. of Cambridge); Robert N.M. Watson (Univ. of Cambridge); Jonathan Anderson (Memorial Univ.); David Chisnall (Univ. of Cambridge); Brooks Davis (SRI International); Ben Laurie (Google UK Ltd.); Ilias Marinos (Univ. of Cambridge); Peter G. Neumann (SRI International); Alex Richardson (Univ. of Cambridge)*	
6:30 – 9:00	Conference Banquet & Award Ceremony (Colorado F – J)			

CCS 2015 MAIN CONFERENCE, THURSDAY OCTOBER 15				
	TRACK A	**TRACK B**	**TRACK C**	**TUTORIAL**
	Room: Denver 1 – 3	**Room: Colorado E**	**Room: Colorado A – D**	**Room: Gold Coin**
6:45 – 8:00	Breakfast and Registration (Colorado Foyer and Central Registration Area)			
	Session 9A Coding, Commitments & Lattices	Session 9B Security-Related Ecosystems	Session 9C Formal Methods Meet Cryptography	
	Session Chair - Rei Safavi-Naini (Univ. of Calgary)	Session Chair - Amir Herzberg (Bar-Ilan Univ.)	Session Chair – Ralph Kuesters (Univ. of Trier)	
8:15 – 8:40	Falcon Codes: Fast, Authenticated LT Codes (Or: Making Rapid Tornadoes Unstoppable) *Ari Juels (Cornell Tech); James Kelley (NetApp); Roberto Tamassia (Brown Univ.); Nikos Triandopoulos (RSA Laboratories & Boston Univ.)*	Drops for Stuff: An Analysis of Reshipping Mule Scams *Shuang Hao (UC Santa Barbara); Kevin Borgolte (UC Santa Barbara); Nick Nikiforakis (Stony Brook University); Gianluca Stringhini (University College London); Manuel Egele (Boston University); Michael Eubanks (Federal Bureau of Investigation); Brian Krebs (KrebsOnSecurity.com); Giovanni Vigna (UC Santa Barbara & Lastline Inc.)*	Equivalence-based Security for Querying Encrypted Databases: Theory and Application to Privacy Policy Audits *Omar Chowdhury (Purdue Univ.); Deepak Garg (Max Planck Institute for Software Systems); Limin Jia (Carnegie Mellon Univ.); Anupam Datta (Carnegie Mellon Univ.)*	Introduction to Cryptocurrencies — *Stefan Dziembowski (University of Warsaw*
8:40 – 9:05	Fast Non-Malleable Commitments *Hai Brenner (IDC Herzliya); Vipul Goyal (Microsoft Research, Bangalore); Silas Richelson (UCLA); Alon Rosen (IDC Herzliya); Margarita Vald (Tel Aviv Univ.)*	Android Root and its Providers: A Double-Edged Sword *Hang Zhang (Univ. of California, Riverside); Dongdong She (Univ. of California, Riverside); Zhiyun Qian (Univ. of California, Riverside)*	Automated Symbolic Proofs of Observational Equivalence *David Basin (ETH Zurich); Jannik Dreier (ETH Zurich); Ralf Sasse (ETH Zurich)*	
9:05 – 9:30	White-Box Cryptography Revisited: Space-Hard Ciphers *Andrey Bogdanov (Technical Univ. of Denmark); Takanori Isobe (Sony Corporation)*	An Empirical Study of Web Vulnerability Discovery Ecosystems *Mingyi Zhao (Pennsylvania State Univ.); Jens Grossklags (Pennsylvania State Univ.); Peng Liu (Pennsylvania State Univ.)*	Automated Proofs of Pairing-Based Cryptography *Gilles Barthe (IMDEA Software Institute); Benjamin Grégoire (INRIA); Benedikt Schmidt (IMDEA Software Institute)*	

	TRACK A	TRACK B	TRACK C	TUTORIAL
	Room: Denver 1 – 3	**Room: Colorado E**	**Room: Colorado A – D**	**Room: Gold Coin**
	Session 9A Coding, Commitments & Lattices	Session 9B Security-Related Ecosystems	Session 9C Formal Methods Meet Cryptography	Introduction to Cryptocurrencies — *Stefan Dziembowski (University of Warsaw*
	Session Chair - Rei Safavi-Naini (Univ. of Calgary)	Session Chair - Amir Herzberg (Bar-Ilan Univ.)	Session Chair – Ralph Kuesters (Univ. of Trier)	
9:30 – 9:55	Lattice Basis Reduction Attack against Physically Unclonable Functions *Fatemeh Ganji (Technische Universität Berlin); Juliane Krämer (Technische Universität Darmstadt); Jean-Pierre Seifert (Technische Universität Berlin); Shahin Tajik (Technische Universität Berlin)*	The Dropper Effect: Insights into Malware Distribution with Downloader Graph Analytics *Bum Jun Kwon (Univ. of Maryland); Jayanta Mondal (Univ. of Maryland); Jiyong Jang (IBM Research, Yorktown Heights); Leyla Bilge (Symantec Research Labs, France); Tudor Dumitra_ (Univ. of Maryland)*	Moat: Verifying Confidentiality of Enclave Programs *Rohit Sinha (Univ. of California, Berkeley); Sriram Rajamani (Microsoft Research); Sanjit Seshia (Univ. of California, Berkeley); Kapil Vaswani (Microsoft Research)*	
10:00 – 10:20	Coffee Break			
	Session 10A Key Exchange: Theory & Practice	Session 10B Mobile Device Attacks	Session 10C Statistical Privacy	
	Session Chair - Stefan Katzenbeisser (TU Darmstadt)	Session Chair - Konstantin Beznosov (U of Brit. Columbia)	Session Chair – Ting Yu (Qatar Computing Research Inst.)	Introduction to Cryptocurrencies — *Stefan Dziembowski (University of Warsaw*
10:30 – 10:55	On the Security of TLS 1.3 and QUIC Against Weaknesses in PKCS#1 v1.5 Encryption *Tibor Jager (Ruhr Univ. Bochum); Jörg Schwenk (Ruhr Univ. Bochum); Juraj Somorovsky (Ruhr Univ. Bochum)*	From System Services Freezing to System Server Shutdown in Android: All You Need Is a Loop in an Application *Heqing Huang (The Pennsylvania State Univ.); Sencun Zhu (The Pennsylvania State Univ.); Kai Chen (Chinese Academy of Sciences); Peng Liu (The Pennsylvania State Univ.)*	Differential Privacy with Bounded Priors: Reconciling Utility and Privacy in Genome-Wide Association Studies *Florian Tramèr (EPFL); Zhicong Huang (EPFL); Erman Ayday (Bilkent Univ.); Jean-Pierre Hubaux (EPFL)*	

	TRACK A	TRACK B	TRACK C	TUTORIAL
	Room: Denver 1 – 3	Room: Colorado E	Room: Colorado A – D	Room: Gold Coin
	Session 10A Key Exchange: Theory & Practice	Session 10B Mobile Device Attacks	Session 10C Statistical Privacy	
	Session Chair - Stefan Katzenbeisser (TU Darmstadt)	Session Chair - Konstantin Beznosov (U of Brit. Columbia)	Session Chair – Ting Yu (Qatar Computing Research Inst.)	
10:55 – 11:20	A Cryptographic Analysis of the TLS 1.3 Handshake Protocol Candidates *Benjamin Dowling (Queensland Univ. of Technology); Marc Fischlin (Technische Universität Darmstadt); Felix Günther (Technische Universität Darmstadt); Douglas Stebila (Queensland Univ. of Technology)*	Hare Hunting in the Wild Android: A Study on the Threat of Hanging Attribute References *Yousra Aafer (Syracuse Univ.); Nan Zhang (Indiana Univ. Bloomington); Zhongwen Zhang (Institute of Information Engineering, Chinese Academic of Sciences); Xiao Zhang (Syracuse Univ.); Kai Chen (Indiana Univ. Bloomington, Chinese Academy of Sciences); XiaoFeng Wang (Indiana Univ. Bloomington); Xiaoyong Zhou (Samsung Research America); Wenliang Du (Syracuse Univ.); Michael Grace (Samsung Research America)*	Protecting Locations with Differential Privacy under Temporal Correlations *Yonghui Xiao (Emory Univ.); Li Xiong (Emory Univ.)*	
11:20 – 11:45	Deniable Key Exchanges for Secure Messaging *Nik Unger (Univ. of Waterloo); Ian Goldberg (Univ. of Waterloo)*	Perplexed Messengers from the Cloud: Automated Security Analysis of Push-Messaging Integrations *Yangyi Chen (Indiana Univ. Bloomington); Tongxin Li (Peking Univ.); XiaoFeng Wang (Indiana Univ. Bloomington); Kai Chen (Indiana Univ. Bloomington and Institute of Information Engineering, CAS); Xinhui Han (Peking Univ.)*	Privacy-Preserving Deep Learning *Reza Shokri (Univ. of Texas at Austin); Vitaly Shmatikov (Cornell Tech)*	
11:45 – 12:10	TOPAS --- 2-Pass Key Exchange with Full Perfect Forward Secrecy and Optimal Communication Complexity *Sven Schäge (Ruhr-Universität Bochum)*	When Good Becomes Evil: Keystroke Inference with Smartwatch *Xiangyu Liu (The Chinese Univ. of Hong Kong); Zhe Zhou (The Chinese Univ. of Hong Kong); Wenrui Diao (The Chinese Univ. of Hong Kong); Zhou Li (ACM Member); Kehuan Zhang (The Chinese Univ. of Hong Kong)*	Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures *Matt Fredrikson (Carnegie Mellon Univ.); Somesh Jha (Univ. of Wisconsin); Thomas Ristenpart (Cornell Tech)*	
12:15 – 1:45	Lunch (Colorado F – J)			

	TRACK A	TRACK B	TRACK C	TUTORIAL
	Room: Denver 1 – 3	Room: Colorado E	Room: Colorado A – D	Room: Gold Coin
	Session 11A Privacy-Preserving Authentication	Session 11B Web Attacks	Session 11C Surveillance and Countermeasures	
	Session Chair - Kui Ren (Univ. of Buffalo)	Session Chair - Michael Franz (Univ. of California, Irvine)	Session Chair - Prateek Mittal (Princeton Univ.)	
1:45 – 2:10	Group Signatures with Probabilistic Revocation: A Computationally-Scalable Approach for Providing Privacy-Preserving Authentication *Vireshwar Kumar (Virginia Tech); He Li (Virginia Tech); Jung-Min (Jerry) Park (Virginia Tech); Kaigui Bian (Peking Univ.); Yaling Yang (Virginia Tech)*	The Clock is Still Ticking: Timing Attacks in the Modern Web *Tom Van Goethem (KU Leuven); Wouter Joosen (KU Leuven); Nick Nikiforakis (Stony Brook Univ.)*	Mass-surveillance without the State: Strongly Undetectable Algorithm-Substitution Attacks *Mihir Bellare (UCSD); Joseph Jaeger (UCSD); Daniel Kane (UCSD)*	
2:10 – 2:35	Authenticating Privately over Public Hotspots *Aldo Cassola (Northeastern Univ. & Univ. San Francisco de Quito); Erik-Oliver Blass (Airbus Group Innovations & Northeastern Univ.); Guevara Noubir (Northeastern Univ.)*	Cross-Site Search Attacks *Nethanel Gelernter (Bar-Ilan Univ.); Amir Herzberg (Bar-Ilan Univ.)*	HORNET: High-speed Onion Routing at the Network Layer *Chen Chen (ETH Zurich & Carnegie Mellon Univ.); Daniele E. Asoni (ETH Zurich); David Barrera (ETH Zurich); George Danezis (Univ. College London); Adrian Perrig (ETH Zurich);*	
2:35 – 3:00	SPRESSO: A Secure, Privacy-Respecting Single Sign-On System for the Web *Daniel Fett (Univ. of Trier); Ralf Kuesters (Univ. of Trier); Guido Schmitz (Univ. of Trier)*	The Spy in the Sandbox: Practical Cache Attacks in Javascript and their Implications *Yossef Oren (Columbia Univ.); Vasileios P. Kemerlis (Columbia Univ.); Simha Sethumadhavan (Columbia Univ.); Angelos D. Keromytis (Columbia Univ.)*	Caronte: Detecting Location Leaks for Deanonymizing Tor Hidden Services *Srdjan Matic (Universita degli Studi di Milano); Platon Kotzias (IMDEA Software Institute); Juan Caballero (IMDEA Software Institute)*	
3:00 – 3:25	Automating Fast and Secure Translations from Type-I to Type-III Pairing Schemes *Joseph A. Akinyele (Johns Hopkins Univ.); Christina Garman (Johns Hopkins Univ.); Susan Hohenberger (Johns Hopkins Univ.)*	From Facepalm to Brain Bender: Exploring Client-Side Cross-Site Scripting *Ben Stock (FAU Erlangen-Nuremberg); Stephan Pfistner (SAP SE); Bernd Kaiser (FAU Erlangen-Nuremberg); Sebastian Lekies (Ruhr-Univ. Bochum); Martin Johns (SAP SE)*	(Un)linkable Pseudonyms for Governmental Databases *Jan Camenisch (IBM Research Zurich); Anja Lehmann (IBM Research Zurich)*	
3:30 – 4:00	Coffee Break (Colorado Foyer)			

	TRACK A	TRACK B	TRACK C	TUTORIAL
	Room: Denver 1 – 3	Room: Colorado E	Room: Colorado A – D	Room: Gold Coin
	Session 12A Outsourcing Data & Computation	Session 12B Cloud, Web & Authentication	Session 12C Side Channel	
	Session Chair - Nick Triandopoulos (RSA Lab & Boston Univ.)	Session Chair - Kehuan Zhang (Chinese Univ. of Hong Kong)	Session Chair - Kun Sun (College of William & Mary)	
4:00 – 4:25	IntegriDB: Verifiable SQL for Outsourced Databases *Yupeng Zhang (Univ. of Maryland); Jonathan Katz (Univ. of Maryland); Charalampos Papamanthou (Univ. of Maryland)*	Maneuvering Around Clouds: Bypassing Cloud-based Security Providers *Thomas Vissers (KU Leuven); Tom Van Goethem (KU Leuven); Wouter Joosen (KU Leuven); Nick Nikiforakis (Stony Brook Univ.)*	Observing and Preventing Leakage in MapReduce *Olga Ohrimenko (Microsoft Research); Manuel Costa (Microsoft Research); Cédric Fournet (Microsoft Research); Christos Gkantsidis (Microsoft Research); Markulf Kohlweiss (Microsoft Research) Divya Sharma (Carnegie Mellon University)*	
4:25 – 4:50	A Domain-Specific Language for Low-Level Secure Multiparty Computation Protocols *Peeter Laud (Cybernetica AS); Jaak Randmets (Cybernetica AS & Univ. of Tartu)*	The SICILIAN Defense: Signature-based Whitelisting of Web JavaScript *Pratik Soni (National Univ. of Singapore); Enrico Budianto (National Univ. of Singapore); Prateek Saxena (National Univ. of Singapore)*	Mitigating Storage Side Channels Using Statistical Privacy Mechanisms *Qiuyu Xiao (Univ. of North Carolina at Chapel Hill); Michael K. Reiter (Univ. of North Carolina at Chapel Hill); Yinqian Zhang (The Ohio State Univ.)*	
4:50 – 5:15	Automated Synthesis of Optimized Circuits for Secure Computation *Daniel Demmler (TU Darmstadt); Ghada Dessouky (TU Darmstadt); Farinaz Koushanfar (Rice Univ.); Ahmad-Reza Sadeghi (TU Darmstadt); Thomas Schneider (TU Darmstadt); Shaza Zeitouni (TU Darmstadt)*	Seeing Your Face Is Not Enough: An Inertial Sensor-Based Liveness Detection for Face Authentication *Yan LI (Singapore Management Univ.); Yingjiu LI (Singapore Management Univ.); Qiang YAN (Singapore Management Univ.); Hancong KONG (Singapore Management Univ.); Robert H. DENG (Singapore Management Univ.)*	Nomad: Mitigating Arbitrary Cloud Side Channels via Provider-Assisted Migration *Soo-Jin Moon (Carnegie Mellon Univ.); Vyas Sekar (Carnegie Mellon Univ.); Michael Reiter (Univ. of North Carolina at Chapel Hill)*	
5:15 – 5:40	Using Linearly-Homomorphic Encryption to Evaluate Degree-2 Functions on Encrypted Data *Dario Catalano (Univ. of Catania); Dario Fiore (IMDEA Software Institute)*		Thwarting Memory Disclosure with Efficient Hypervisor-enforced Intra-domain Isolation *Yutao Liu (Shanghai Jiao Tong Univ.); Tianyu Zhou (Shanghai Jiao Tong Univ.); Kexin Chen (Shanghai Jiao Tong Univ.); Haibo Chen (Shanghai Jiao Tong Univ.); Yubin Xia (Shanghai Jiao Tong Univ.)*	
5:40 – 6:00	CCS 2015 MAIN CONFERENCE CLOSING & VOTE OF THANKS			

Post-conference Workshops
October 16, 2015

Please check monitors for last minute changes to room assignments

7th ACM CCS International Workshop on Managing Insider Security Threats (MIST 2015)	
6:45 – 8:00	Breakfast and Registration (Colorado Foyer and Central Registration Area)
8:00 – 8:55	Opening Remarks & Logistics – MIST 2015 meets in Colorado G
8:55 – 9:55	**Technical Session 1, Session Chair: Fang-Yie Leu**
	Insider Threats: Identifying Anomalous Human Behavior in Heterogeneous Systems Using Beneficial Intelligent Software (Benware) *Andrew Stephen McGough, David Wall, John Brennan, George Theodoropoulos, Ed Ruck-Keene (Durham University), Budi Arief, Carl Gamble, John Fitzgerald, Aad van Moorsel (Newcastle University) and Sujeewa Alwis (Insighlytics Ltd.)*
	Detecting Insider Threat from Enterprise Social and Online Activity Data *Gaurang Gavai, Kumar Sricharan, Dave Gunning, Rob Rolleston, John Hanley, Mudita Singhal (Palo Alto Research Center)*
	Modelling Social-Technical Attacks with Timed Automata *Nicolas David (University of Nantes/LINA), Alexandre David, René Rydhof Hansen, Kim G. Larsen (Aalborg University), Axel Legay (INRIA), Mads Chr. Olesen (Aalborg University), Christian W. Probst (Technical University of Denmark)*
	Novel Insider Threat Techniques: Automation and Generation of Ad Hoc Digital Evidence *Aniello Castiglione, Arcangelo Castiglione, Alfredo De Santis, Barbara Masucci, Francesco Palmieri, Raffaele Pizzolante (University of Salerno)*
	Mobile App Security Assessment with the MAVeriC Dynamic Analysis Module Alessandro Armando *(University of Genoa), Gianluca Bocci (Poste Italiane), Gabriele Costa (University of Genoa), Rocco Mammoliti (Poste Italiane), Alessio Merlo (University of Genoa), Silvio Ranise, Riccarto Traverso (Bruno Kessler Foundation), Andrea Valenza (University of Genoa)*
10:45 – 11:10	Coffee Break (Colorado Foyer)
11:10 – 12:30	**Keynote Speech**: Detecting Insider Threats: Who is Winning the Game? William R. Claybomb (Carnegie Melon University) Session Chair: Christian W. Probst
12:30 – 2:00	Lunch
2:00 – 3:40	**Technical Session – Best Paper and Poster; Session Chair: Kyung Hyun Rhee**
	Compliance Control: Managed Vulnerability Surface in Social-Technological Systems via Signaling Games *William Casey (Carnegie Mellon University), Quanyan Zhu (New York University), Jose Andre Morales (Carnegie Mellon University), Bud Mishra (New York University)*
	Secure Power Management Scheme for WSN *Kun-Lin Tsai, Meng Yuan Ye, Fang-Yie Leu (Tunghai University)*
	SKETURE: A Sketch-based Packet Analysis Tool *Sherenaz Al-Haj Baddar (University of Jordan), Alessio Merlo (University of Genoa) Mauro Migliardi (University of Padua)*
	Towards Insider Threat Detection Using Psychophysiological Signals *Yessir Hashem, Hassan Takabi, Mohammad GhasemiGol, Ram Dantu (University of North Texas)*
	A Preliminary Cyber Ontology for Insider Threats in the Financial Sector *Gökhan Kul, Shambhu Upadhyaya (The State University of New York at Buffalo)*
3:40 – 4:00	Coffee Break (Colorado Foyer)
4:00 – 6:00	**Panel Discussion**: Cyber Threats to Industrial Control Systems; Session Chair: Kangbin Yim Yim Kangbin Yim (Soonchunhyang University), Aniello Castiglione *(University of Salerno), Jeong Hyun Yi (Soongsil University), Mauro Migliardi (University of Padua), Ilsun You (Soonchunhyang University)*
End of International Workshop on Managing Insider Security Threats	

7th ACM Cloud Computing Security Workshop (CCSW 2015)	
6:45 – 8:00	Breakfast and Registration (Colorado Foyer and Central Registration Area)
8:00 – 8:55	Opening Remarks & Logistics – CCSW meets in Colorado AB
8:55 – 9:55	**Keynote Speech**: Side-Channels in Multi-Tenant Environments; Mike Reiter (University of North Carolina)
9:55 – 10:45	**Technical Session – System Security, Session Chair: Rei Sefavi-Naini**
	How Private is Your Private Cloud? - Security Analysis of Cloud Control Interfaces *Dennis Felsch (Ruhr-University Bochum); Mario Heiderich (Ruhr-University Bochum); Frederic Schulz (Ruhr-University Bochum); Jörg Schwenk (Ruhr-University Bochum)*
	Return Of The Covert Channel, Data Center Style *Ken Block (Northeastern University); Guevara Noubir (Northeastern University)*
10:45 – 11:10	Coffee Break (Colorado Foyer)
11:10 – 12:10	**Keynote Speech**: Cloud Security: The Industry Landscape and the Lure of Zero-Knowledge Protection Chenxi Wang (Twistlock)
12:30 – 2:00	Lunch
2:00 – 2:50	**Keynote Speech**: Being Successful in the Cloud - Special secret or just plain old logic; Bruce Grenfell (Concur / SAP)
2:50 – 3:40	**Technical Session – Applied Cryptography I, Session Chair: Aniket Kate**
	Performance Analysis of Linux RNG in Virtualized Environments *Rashmi Kumari (University of Calgary); Mohsen Alimomeni (University of Calgary); Reihaneh Safavi Naini (University of Calgary)*
	Fast Order-Preserving Encryption from Uniform Distribution Sampling *Yong Ho Hwang (Samsung); Sungwook Kim (Samsung); Jae Woo Seo (Samsung)*
3:40 – 4:00	Coffee Break (Colorado Foyer)
4:00 – 4:50	**Technical Session – Applied Cryptography II, Session Chair: Marten van Dijk**
	Exploring Privacy Preservation in Outsourced K-Nearest Neighbors with Multiple Data Owners *Frank Li (Univ. of California Berkeley); Eui Chul Richard Shin (Univ. of California Berkeley); Vern Paxson (UC Berkeley / ICSI)*
	ORAM based forward privacy preserving Dynamic Searchable Symmetric Encryption Schemes *Panagiotis Rizomiliotis (University of the Aegean); Stefanos Gritzalis (University of the Aegean)*
End of Cloud Computing Security Workshop	

8th ACM Workshop on Artificial Intelligence and Security (AISec 2015)	
6:45 – 8:00	Breakfast and Registration (Colorado Foyer and Central Registration Area)
8:00 – 9:00	Opening Remarks & Logistics – AISec 2015 meets in Colorado C
9:00 – 10:00	**Keynote Speech**: Machine Learning for Enterprise Security; Pratyusa Manadhata
10:00 – 10:45	**Technical Session – Malware and Malicious Activity**
	Detecting Malicious Network Activities on Android Through Scalable Triggering Relation Discovery (presentation only) *Hao Zhang, Danfeng Yao and Naren Ramakrishnan*
	Malicious Behavior Detection using Windows Audit Logs *Konstantin Berlin, David Slater and Joshua Saxe*
10:45 – 11:10	Coffee Break (Colorado Foyer)
11:10 – 12:30	Better Malware Ground Truth: Techniques for Weighting Anti-Virus Vendor Labels *Alex Kantchelian, Michael Carl Tschantz, Sadia Afroz, Brad Miller, Anthony Joseph, J. D. Tygar, Vaishaal Shankar and Rekha Bachwani*
	Remote operating system classification over IPv6 *David Fifield, Alexandru Geana, Luis Martingarcia, Mathias Morbitzer and J. D. Tygar*
12:30 – 2:00	Lunch
2:00 – 3:40	**Technical Session – Adversarial Learning and Social Networks**
	Scalable Optimization of Randomized Operational Decisions in Adversarial Classification Settings (presentation only) *Bo Li and Yevgeniy Vorobeychik*
	Automated Attacks on Compression-Based Classifiers *Igor Burago and Daniel Lowd*
	Know thy Victim, Fight thy Foe: Thwarting Fake OSN Accounts by Predicting their Victims *Yazan Boshmaf, Matei Ripeanu and Konstantin Beznosov*
	Detecting Clusters of Fake Accounts in Online Social Networks *Cao Xiao, David Mandell Freeman and Theodore Hwa*
3:40 – 4:00	Coffee Break (Colorado Foyer)
4:00 – 5:15	**Technical Session – Privacy, Learning and Security**
	Fast, Privacy Preserving Linear Regression over Distributed Datasets based on Pre-Distributed Data *Martine de Cock, Rafael Dowsley, Anderson Nascimento and Stacey Newman*
	Differential Privacy for Classifier Evaluation *Kendrick Boyd, Eric Lantz and David Page*
	Subsampled Exponential Mechanism: Differential Privacy in Large Output Spaces *Eric Lantz, Kendrick Boyd and David Page*
End of Workshop on Artificial Intelligence and Security	

1st ACM Workshop on Cyber Physical Systems Security and Privacy (CPS-SPC 2015)	
6:45 – 8:00	Breakfast and Registration (Colorado Foyer and Central Registration Area)
8:00 – 9:00	Opening Remarks & Logistics – CPS-SPC 2015 meets in Colorado H
9:00 – 10:30	**Technical Session - Miscellaneous**
	On Passive Data Link Layer Fingerprinting of Aircraft Transponders *Martin Strohmeier (University of Oxford) and Ivan Martinovic (University of Oxford)*
	Eliminating Inter-Domain Vulnerabilities in Cyber-Physical Systems: An Analysis Contracts Approach *Ivan Ruchkin (Carnegie Mellon University), Ashwini Rao (Carnegie Mellon University) Dionisio De Niz (Software Engineering Institute), Sagar Chaki (Software Engineering Institute) and David Garlan (Carnegie Mellon University)*
	The Impact of Social Engineering on Industrial Control System Security *Benjamin Green (Lancaster University), Daniel Prince (Lancaster University), Jerry Busby (Lancaster University) and David Hutchison (Lancaster University*
10:45 – 11:10	Coffee Break (Colorado Foyer)
11:10 – 12:30	**Technical Session - Control and Theoretical Foundations**
	Secure and Resilient Control Design for Cloud Enabled Networked Control Systems *Zhiheng Xu (New York University) and Quanyan Zhu (New York University)*
	Attack Mitigation in Adversarial Platooning Using Detection-Based Sliding Mode Control *Imran Sajjad (Utah State University), Daniel D. Dunn (Utah State University), Rajnikant Sharma (Utah State University) and Ryan Gerdes (Utah State University)*
	Scheduling Intrusion Detection Systems in Resource-Bounded Cyber-Physical Systems *Waseem Abbas (Vanderbilt University), Aron Laszka (Vanderbilt University), Yevgeniy Vorobeychik (Vanderbilt University) and Xenofon Koutsoukos (Vanderbilt University)*
12:30 – 2:00	Lunch
2:00 – 3:40	**Technical Session - Testbeds, Simulations and Requirements**
	Secure RTOS Architecture for Building Automation *Xiaolong Wang (Kansas State University), Masaaki Mizuno (Kansas State University), Mitch Neilsen (Kansas State University), Xinming Ou (University of South Florida), S. Raj Rajagopalan (Honeywell ACS Labs), Will G. Baldwin (Biosecurity Research Institute) and Bryan Phillips (Biosecurity Research Institute)*
	MiniCPS: A toolkit for security research on CPS Networks *Daniele Antonioli (Singapore University of Technology and Design) and Nils Tippenhauer (Singapore University of Technology and Design)*
	A Real-Time Testbed Environment for Cyber-Physical Security on the Power Grid *Georgia Koutsandria (University of Rome La Sapienza), Reinhard Gentz (Arizona State University), Mahdi Jamei (Arizona State University), Anna Scaglione (Arizona State University), Sean Peisert (Lawrence Berkeley National Laboratory and University of California Davis) and Chuck McParland (Lawrence Berkeley National Laboratory)*
3:40 – 4:00	Coffee Break (Colorado Foyer)
4:00 – 5:00	**Technical Session - Security Assurance and Assessment**
	Assurance Techniques for Industrial Control Systems (ICS) *William Knowles (Lancaster University), Jose Such (Lancaster University), Antonios Gouglidis (Lancaster University), Gaurav Misra (Lancaster University) and Awais Rashid (Lancaster University)*
	A Field Study of Digital Forensics of Intrusions in the Electrical Power Grid *Eli Sohl (Western Washington University), Curtis Fielding (Western Washington University), Tyler Hanlon (Western Washington University), Julian Rrushi (Western Washington University), Hassan Farhangi (British Columbia Inst. of Tech.), Clay Howey (British Columbia Inst. of Tech.), Kelly Carmichael (British Columbia Inst. of Tech.) and Joey Dabell (British Columbia Inst. of Tech.)*
5:00 – 5:45	**Discussion on the future organization and directions for the workshop**
End of Workshop on Cyber Physical Systems Security and Privacy	

International Workshop on Trustworthy Embedded Devices (TrustED 2015)	
6:45 – 8:00	Breakfast and Registration (Colorado Foyer and Central Registration Area)
8:00 – 8:20	Opening Remarks & Logistics – TrustED 2015 meets in Colorado D
8:25 – 10:50	**Technical Session – Hardware Security I**
	Invited Talk - Hardware Security and its adversaries *Marten van Dijk (University of Connecticut)*
	Characterizing Composite User-Device Touchscreen Physical Unclonable Functions (PUFs) for Mobile Device Authentication *Ryan Scheel (Iowa State University); Akhilesh Tyagi (Iowa State University)*
	On the Systematic Drift of Physically Unclonable Functions *Andre Schaller (TU Darmstadt); Boris Skoric (Eindhoven University of Technology); Stefan Katzenbeisser (TU Darmstadt)*
	Faster Leakage Detection and Exploitation *Xin Ye (Worcester Polytechnic Institute); Cong Chan (Worcester Polytechnic Institute); Mostafa Taha (Assiut University); Thomas Eisenbarth (Worcester Polytechnic Institute*)
10:45 – 11:10	Coffee Break (Colorado Foyer)
11:10 – 12:30	**Technical Session – Hardware Security II**
	Security-Aware Design Flow for 2.5D IC Technology *Yang Xie (University of Maryland); Chongxi Bao (University of Maryland); Ankur Srivastava (University of Maryland)*
	Invited Talk: A Plea for Incremental Work in IoT Security Geremy Condra (Google)
12:30 – 2:00	Lunch
2:00 – 3:40	**Technical Session – System Security I**
	Invited Talk - Leveraging Processor Performance Counters for Security and Performance *Jakub Szefer (Yale University)*
	Content Protection in HTML5 TV Platforms: towards Browser-agnostic DRM and Cloud UI environments *Alexandra Mikityuk (TU Berlin, Deutsche Telekom AG); Stefan Pham (TU Berlin); Stefan Kaiser (TU Berlin); Oliver Friedrich (Deutsche Telekom AG); Stefan Arbanowski (TU Berlin)*
3:40 – 4:00	Coffee Break (Colorado Foyer)
4:00 – 5:20	**Technical Session – System Security II**
	Invited Talk - An Overview of Automotive Cybersecurity: Challenges and Solution Approaches *Andre Weimerskirch (University of Michigan)*
	XNPro: Low-Impact Hypervisor-Based Execution Prevention in ARM *Jan Nordholz (TU Berlin); Julian Vetter (TU Berlin); Michael Peter (TU Berlin); Matthias Petschick (TU Berlin); Janis Danisevskis (TU Berlin)*
5:20 – 5:30	**Adjourn**
End of International Workshop on Trustworthy Embedded Devices	

ACM CCS 2015 Sponsors & Supporters

Sponsor

Supporters

U.S.Army
Research Office

Microsoft Research

IBM Research

Colorado State University

ASU