

ACM ASIACCS 2018



The 13th ACM ASIA Conference on Information, Computer and Communications Security
June 4 - 8, 2018, Songdo, Korea

Monday, June 4 Pre-Conference Workshops

Time	Workshop on Blockchains, Cryptocurrencies and Contracts (BCC)	Cyber-Physical System Security Workshop (CPSS)	Radical and Experiential Security Workshop (RESEC)	International Workshop on Security in Cloud Computing (SCC)	ASIA Public-Key Cryptography Workshop (APKC)	
09:00 - 10:30	BCC	CPSS	RESEC	SCC		
10:30 - 11:00	Coffee Break					
11:00 - 12:30	BCC	CPSS	RESEC	SCC		
12:30 - 14:00	Lunch					
14:00 - 15:30	BCC	CPSS	RESEC	SCC	APKC 13:25 ~ 18:00	
15:30 - 16:00	Coffee Break					
16:00 - 17:30	BCC	CPSS	RESEC	SCC		

Tuesday, June 5 AsiaCCS Main Conference

Time	Diamond Hall (2F)	Ruby Hall (2F) Research Track 1	Emerald Hall (2F) Research Track 2	Sapphire Hall (3F) Tutorial, Invited, Sponsor Talk
09:00 - 09:30	Welcome Message (General Chair/Program Committee Chair)			
09:30 - 10:30	Keynote Cliff Wang (US Army Research) "Cyber Deception: an emergent research area"			
10:30 - 11:00	Coffee Break			
11:00 - 12:20		Embedded System Security DeWiCam: Detecting Hidden Wireless Cameras via Smartphones Yushi Cheng, Xiaoyu Ji (Zhejiang University/Alibaba-Zhejiang University Joint Institute of Frontier Technologies); Tianyang Lu, and Wenyuan Xu (Zhejiang University) Leaky Wires: Information Leakage and Covert Communication Between FPGA Long Wires Ilias Giechaskiel, Kasper B. Rasmussen (University of Oxford); and Ken Eguro (Microsoft Research) HicAuth: Key-free and Secure Communications via Home-Limited Channel Chaohao Li, Xiaoyu Ji (Zhejiang University & Alibaba-Zhejiang University Joint Institute of Frontier Technologies); Xinyan Zhou, Juchuan Zhang (Zhejiang University); Jing Tian (University of South Carolina); Yanmiao Zhang, and Wenyuan Xu (Zhejiang University)	Applied Crypto 1 Ciphertext Integrity with Misuse and Leakage: Definition and Efficient Constructions with Symmetric Primitives Francesco Berti, François Koeune, Olivier Pereira, Thomas Peters, and François-Xavier Standaert (Universite Catholique de Louvain) On the Memory-Hardness of Data-Independent Password-Hashing Functions Joel Alwen (IST Austria / Wickr Inc.); Peter Gazi (IOHK); Chethan Kamath, Karen Klein, Georg Osang, Krzysztof Pietrzak (IST Austria); Lenoid Reyzin (Boston University); Michal Rolinek, and Michal Rybar (IST Austria) Non-interactive and Output Expressive Private Comparison from Homomorphic Encryption and the Applications Wen-jie Lu, Jun-jie Zhou, and Jun Sakuma (University of Tsukuba)	Invited Talk 1: Using Text Analytics to Enhance Security Analysis of Mobile Applications, William Enck (NC State) 11:00 – 12:00
12:20 - 13:50	Lunch			
13:50 - 15:20		Authentication	Mobile	

	<p>The Personal Identification Chord: A Four Button Authentication System for Smartwatches Ian Oakley (UNIST); Jun Ho Huh (Samsung Electronics); Junsung Cho, Geumhwan Cho (Sungkyunkwan University); Rasel Islam (UNIST); and Hyounghick Kim (Sungkyunkwan University)</p> <p>2MA: Verifying Voice Commands via Two Microphone Authentication Logan Blue, Hadi Abdullah, Luis Vargas, and Patrick Traynor (University of Florida)</p> <p>Beat-PIN: A User Authentication Mechanism for Wearable Devices Through Secret Beats Ben Hutchins, Anudeep Reddy, Wenqiang Jin, Michael Zhou, Ming Li, and Lei Yang (University of Nevada, Reno)</p>	<p>iOracle: Automated Evaluation of Access Control Policies in iOS Luke Deshotels (North Carolina State University); Razvan Deaconescu, Costin Carabas, Iulia Manda (University POLITEHNICA of Bucharest); William Enck (North Carolina State University); Mihai Chiroiu (University POLITEHNICA of Bucharest); Ninghui Li (Purdue University); and Ahmad-Reza Sadeghi (Technische Universitat Darmstadt)</p> <p>Source Attribution of Cryptographic API Misuse in Android Applications Ildar Muslukhov (The University of British Columbia); Yazan Boshmaf (Qatar Computing Research Institute); and Konstantin Beznosov (The University of British Columbia)</p> <p>Don't throw me away: Threats Caused by the Abandoned Internet Resources Used by Android Apps Elkana G Pariwono (Waseda University); Daiki Chiba, Mitsuaki Akiyama (NTT Secure Platform Laboratories); and Tatsuya Mori (Waseda University)</p>	<p>Tutorial Talk 1: Understanding and Solving the Privacy Challenges in the Smart City Speakers: Dr. David Eckhoff (TUMCREATE) and Isabel Wagner (De Montfort Univ.) 13:50 – 17:40</p>
15:20 - 15:50	Coffee Break		
15:50 - 17:40	<p>Machine Learning 1</p> <p>Protecting Intellectual Property of Deep Neural Networks with Watermarking Jialong Zhang, Zhongshu Gu, Jiyong Jang, Hui Wu, Marc P Stoecklin, Heqing Huang, and Ian M Molloy (IBM Research)</p> <p>Towards Fast and Semi-supervised Identification of Smart Meters launching Data Falsification Attacks Shameek Bhattacharjee, Aditya Thakur, and Sajal K. Das (Missouri University of Science and Technology)</p> <p>Detecting Malicious PowerShell Commands using Deep Neural Networks Danny Hendler (Ben-Gurion University of the Negev); Shay Kels (Microsoft); and Amir Rubin (Ben-Gurion University of the Negev)</p> <p>Detection under Privileged Information Z. Berkay Celik, Patrick McDaniel (penn state); Rauf Izmailov (Vencore Labs); Nicolas Papernot, Ryan Sheatsley, Raquel Alvarez (penn state); and Ananthram Swami (Army Research Laboratory)</p>	<p>Privacy 1</p> <p>Entwining Sanitization and Personalization on Databases Sébastien Gambis (UQAM); Julien Lolive (Universite Rennes 1); and Jean-Marc Robert (ETS)</p> <p>Large-Scale Privacy-Preserving Statistical Computations for Distributed Genome-Wide Association Studies Oleksandr Tkachenko, Christian Weinert, Thomas Schneider, and Kay Hamacher (TU Darmstadt)</p> <p>Secure Similar Sequence Query on Outsourced Genomic Data Ke Cheng, Yantian Hou (Boise State University); and Liangmin Wang (Jiangsu University)</p> <p>A Linear Distinguisher and its Application for Analyzing Privacy-Preserving Transformation Used in Verifiable (Outsourced) Computation Liang Zhao (Sichuan University) and Liquan Chen (University of Surrey)</p>	<p>Tutorial Talk 1: Continue</p>
17:40 - 20:30	Poster Session		
18:30 - 20:30	Welcome Reception		

Wednesday, June 6

AsiaCCS Main Conference

Time	Diamond Hall (2F)	Ruby Hall (2F) Research Track 1	Emerald Hall (2F) Research Track 2	Sapphire Hall (3F) Tutorial, Invited, Sponsor Talk
09:00 - 10:00	Keynote Jaeyeon Jung			
10:00 - 10:30	Coffee Break			
10:30 - 12:30		Cellular, Phone, and Email	Trust	

FBSleuth: Fake Base Station Forensics via Radio Frequency Fingerprinting Zhou Zhuang, Xiaoyu Ji, Taimin Zhang, Juchuan Zhang, Wenyuan Xu (Zhejiang University); Zhenhua Li (Tsinghua University); and Yunhao Liu (Tsinghua University; Michigan State University)	Temporal Consistency of Integrity-Ensuring Computations and Applications to Embedded Systems Security Xavier Carpent (University of California, Irvine); Karim Eldefrawy (SRI International); Norrathep Rattanavipanon, and Gene Tsudik (University of California, Irvine)	Invited Talk 2: T-Fuzz: fuzzing by program transformation, Mathias Payer (Purdue) 10:30 – 11:30
Augmenting Telephone Spam Blacklists by Mining Large CDR Datasets Jienan Liu (University of Georgia); Babak Rahbarinia (Auburn University Montgomery); Roberto Perdisci (University of Georgia); Haitao Du, and Li Su (China Mobile Research Institute)	SALAD: Secure and Lightweight Attestation of Highly Dynamic and Disruptive Networks Florian Kohnhäuser, Niklas Büscher, and Stefan Katzenbeisser (TU Darmstadt)	Sponsor Talk 1: IFAA Powers the Creating of the Online Trusted Identities, Feng, Chunpei (Ant Financial) 11:30 – 12:30
Towards Measuring the Role of Phone Numbers in Twitter-Advertised Spam Payas Gupta (Pindrop); Roberto Perdisci (University of Georgia); and Mustaque Ahamad (Georgia Institute of Technology)	Can You Trust Your Encrypted Cloud? An Assessment of SpiderOakONE's Security Anders P. K. Dalskov and Claudio Orlandi (Aarhus University)	
Use-After-FreeMail: Generalizing the Use-After-Free Problem and Applying it to Email Services Daniel Gruss, Michael Schwarz (Graz University of Technology); Matthias Wübbeling (Fraunhofer FKIE & University of Bonn); Simon Guggi (Graz University of Technology); Timo Malderle (University of Bonn); Stefan More, and Moritz Lipp (Graz University of Technology)	On the strategy and behavior of Bitcoin mining with N-attackers Hanqing Liu, Na Ruan, Rongtian Du, and Weijia Jia (Shanghai Jiao Tong University)	

12:30 - 14:00

Lunch

14:00 - 15:20

Software Security	Network Security 1	
A Leak-Resilient Dual Stack Scheme for Backward-Edge Control-Flow Integrity Philipp Zieris and Julian Horsch (Fraunhofer AISEC)	To Intercept or not to Intercept: Analyzing TLS Interception in Network Appliances Louis Waked, Mohammad Mannan, and Amr Youssef (Concordia University)	Tutorial Talk 2: Recent Trends in Adversarial Machine Learning (AML), Somesh Jha (Univ of Wisconsin, Madison) 14:00 – 15:20
CUP: Comprehensive User-Space Protection for C/C++ Nathan Burow, Derrick McKee, Scott A. Carr, and Mathias Payer (Purdue University)	Software-Defined Firewall: Enabling Malware Traffic Detection and Programmable Security Control Shang Gao, Zecheng Li (Hong Kong Polytechnic University); Yuan Yao (Northwestern Polytechnical University & Hong Kong Polytechnic University); Bin Xiao (Hong Kong Polytechnic University); Songtao Guo (Southwest University); and Yuanyuan Yang (Stony Brook University)	
BCD: Decomposing Binary Code Into Components Using Graph Clustering Vishal M Karande, Swarup Chandra (The University of Texas at Dallas); Zhiqiang Lin (The Ohio State University); Juan Caballero (IMDEA Software Institute); Latifur Khan, and Kevin Hamlen (The University of Texas at Dallas)	Where's Wally? How to Privately Discover your Friends on the Internet Panagiotis Papadopoulos (FORTH-ICS); Antonios A. Chariton (University of Crete); Elias Athanasopoulos (University of Cyprus); and Evangelos P. Markatos (FORTH-ICS)	

15:20 - 15:50

Coffee Break

15:50 - 18:00

Malware and Web	Physical Attacks and Defense	
------------------------	-------------------------------------	--

<p>You Are Your Photographs: Detecting Multiple Identities of Vendors in the Darknet Marketplaces Xiangwen Wang, Peng Peng, Chun Wang, and Gang Wang (Virginia Tech)</p> <p>Investigating Web Defacement Campaigns at Large Federico Maggi, Marco Balduzzi (Trend Micro Italy s.r.l.); Ryan Flores (Forward-looking Threat Research Team); Lion Gu, and Vincenzo Ciancaglini (Trend Micro, Inc.)</p> <p>Hardware Performance Counters Can Detect Malware: Myth or Fact? Boyou Zhou, Anmol Gupta, Rasoul Jahanshahi, Manuel Egele, and Ajay Joshi (Boston University)</p> <p>le-git-imate: Towards Verifiable Web-based Git Repositories Hammad Afzali (New Jersey Institute of Technology); Santiago Torres-Arias (New York University); Reza Curtmola (New Jersey Institute of Technology); and Justin Cappos (New York University)</p>	<p>NoisePrint: Attack Detection Using Sensor and Process Noise Fingerprint in Cyber Physical Systems Chuadry Mujeeb Ahmed (Singapore University of Technology and Design); Martin Ochoa (Singapore University of Technology and Design & Department of Applied Mathematics and Computer Science, Universidad del Rosari); Jianying Zhou, Aditya P. Mathur, Rizwan Qadeer (Singapore University of Technology and Design); Carlos Murguia (Melbourne University); and Justin Ruths (UT Dallas)</p> <p>Electromagnetic Induction Attacks Against Embedded Systems Jayaprakash Selvaraj (Iowa State University); Gokcen Yilmaz Dayanikli (Virginia Tech); Neelam Prabhu Gaunkar (Iowa State University); David Ware (Utah State University); Ryan M Gerdes (Virginia Tech); and Mani Mina (Iowa State University)</p> <p>Sensor CON-Fusion: Defeating Kalman Filter in Signal Injection Attack Shoei Nashimoto, Daisuke Suzuki (Mitsubishi Electric); Takeshi Sugawara, and Kazuo Sakiyama (University of Electro-Communications)</p> <p>TABOR: A Graphical Framework for Anomaly Detection in Industrial Control Systems Qin Lin (Delft University of Technology); Sridha Adepu (Singapore University of Technology and Design); Sicco Verwer (Delft University of Technology); and Aditya Mathur (Singapore University of Technology and Design)</p>	<p>Invited Talk 3: Reconciling Remote Attestation and Safety-Critical Operation on Simple IoT Devices, Gene Tsudik (UC Irvine) 15:50 – 16:50</p> <p>Invited Talk 4: Analog cyber security—from 0101 to mixed signals. Wenyuan Xu (Zhejiang Univ) 16:50 – 17:50</p>
--	---	--

18:00 - 20:30

Poster Session

18:30 - 20:30

Banquet

Thursday, June 7 AsiaCCS Main Conference

Time	Diamond Hall (2F)	Ruby Hall (2F) Research Track 1	Emerald Hall (2F) Research Track 2	Sapphire Hall (3F) Tutorial, Invited, Sponsor Talk
08:30 - 09:30	Keynote Kevin Fu (University of Michigan) “Analog Sensor Cybersecurity and Transduction Attacks”			
09:30 - 09:50	Coffee Break			
09:50 - 11:10		Privacy 2	CPU Security	
		<p>SecSAKE: Towards Secure and Efficient Outsourcing of Clinical MRI Reconstruction Zihao Shan (State University of New York at Buffalo); Zhan Qin (The University of Texas at San Antonio); Leslie Ying, and Kui Ren (State University of New York at Buffalo)</p> <p>Highly-Efficient Fully-Anonymous Dynamic Group Signatures David Derler (Graz University of Technology) and Daniel Slamanig (AIT Austrian Institute of Technology)</p> <p>Direct Anonymous Attestation with Efficient Verifier-Local Revocation for Subscription System Vireshwar Kumar, He Li, Noah Luther, Pranav Asokan, Jung-Min (Jerry) Park (Virginia Tech); Kaigui Bian (Peking University); Martin B. H. Weiss, and Taieb Znati (University of Pittsburgh)</p>	<p>Single Trace Attack against RSA Key Generation in Intel SGX SSL Samuel Weiser, Raphael Spreitzer, and Lukas Bodner (Graz University of Technology)</p> <p>Automated Detection, Exploitation, and Elimination of Double-Fetch Bugs using Modern CPU Features Michael Schwarz, Daniel Gruss, Moritz Lipp (Graz University of Technology); Clémentine Maurice (CNRS, IRISA); Thomas Schuster (Graz University of Technology); Anders Fogh (G DATA Advanced Analytics); and Stefan Mangard (Graz University of Technology)</p> <p>Leveraging Hardware Transactional Memory for Cache Side-Channel Defenses Sanchuan Chen (The Ohio State University); Fangfei Liu (Intel Corporation); Zeyu Mi (Shanghai Jiao Tong University); Yinqian Zhang (The Ohio State University); Ruby B. Lee (Princeton University); Haibo Chen (Shanghai Jiao Tong University); and XiaoFeng Wang (Indiana University at Bloomington)</p>	<p>Invited Talk 5: The Hazards of Coarse Control: Understanding and Protecting Smart Device Control Surfaces, XiaoFeng Wang (Indiana Univ) 09:50 – 10:50</p>

Friday, June 8

AsiaCCS Main Conference

Time	Diamond Hall (2F)	Ruby Hall (2F) Research Track 1 Network Security 2	Emerald Hall (2F) Research Track 2 Applied Crypto 2	Sapphire Hall (3F) Tutorial, Invited, Sponsor Talk
09:00 - 10:50		<p>Cybercrime After the Sunrise: A Statistical Analysis of DNS Abuse in New gTLDs Maciej Korczynski (Grenoble Alps University); Maarten Wullink (SIDN Labs); Samaneh Tajalizadehkhoob (Delft University of Technology); Giovane C. M. Moura (SIDN Labs); Arman Noroozian (Delft University of Technology); Drew Bagley (Secure Domain Foundation / CrowdStrike); and Cristian Hesselman (SIDN Labs)</p> <p>Who is knocking on Telnet Port: A Large-Scale Empirical Study of Network Scanning Hwanjo Heo (KAIST/ETRI) and Seungwon Shin (KAIST)</p> <p>Towards Sustainable Evolution for the TLS Public-Key Infrastructure Taeho Lee, Christos Pappas (ETH Zurich); Pawel Szalachowski (SUTD); and Adrian Perrig (ETH Zurich)</p> <p>No One In The Middle: Enabling Network Access Control Via Transparent Attribution Jeremy Erickson, Qi Alfred Chen, Xiaochen Yu, Erinjen Lin, Robert Levy, and Z. Morley Mao (University of Michigan)</p>	<p>Achieving Flexibility for ABE with Outsourcing via Proxy Re-Encryption Zuoxia Yu (The Hong Kong Polytechnic University); Man Ho Au (The Hong Kong Polytechnic University); Rupeng Yang (Shandong University & The Hong Kong Polytechnic University); Junzuo Lai (Jinan University, Guangzhou & State Key Laboratory of Cryptology); and Qiuliang Xu (Shandong University)</p> <p>Pseudoentropic Isometries: A New Framework for Fuzzy Extractor Reusability Quentin Alamelou, Paul-Edmond Berthier, Chloe Cachet, Stephane Cauchie (equensWorldline); Benjamin Fuller (University of Connecticut); Philippe Gaborit (Universite de Limoges); and Sailesh Simhadri (University of Connecticut)</p> <p>Efficient Two-level Homomorphic Encryption in Prime-order Bilinear Groups and A Fast Implementation in WebAssembly Nuttapong Attrapadung, Goichiro Hanaoka (AIST); Shigeo Mitsunari (Cybozu Labs, Inc.); Yusuke Sakai (AIST); Kana Shimizu (Waseda University); and Tadanori Teruya (AIST)</p> <p>Isogrammic-Fusion ORAM: Improved Statistically Secure Privacy-Preserving Cloud Data Access for Thin Clients Michael T. Goodrich (University of California, Irvine)</p>	
10:50 - 11:20	Coffee Break			
11:20 - 12:50		<p>Chameleon: A Hybrid Secure Computation Framework for Machine Learning Applications Mohammad Sadegh Riazi (University of California San Diego); Christian Weinert, Oleksandr Tkachenko (TU Darmstadt); Ebrahim Mohammadgholi Songhori (University of California San Diego); Thomas Schneider (TU Darmstadt); and Farinaz Koushanfar (University of California San Diego)</p> <p>A Data-driven Attack against Support Vector Machine Shigang Liu, Jun Zhang (Swinburne University of Technology); Yu Wang (Guangzhou University); Wanlei Zhou (Deakin University); Yang Xiang (Swinburne University of Technology); and Olivier De Vel. (Defence Science & Technology Group)</p> <p>Efficient Repair of Polluted Machine Learning Systems via Causal Unlearning Yinzhi Cao (Lehigh University); Alexander Fangxiao Yu, Andrew Aday (Columbia University); Eric Stahl, Jon Merwine (Lehigh University); and Junfeng Yang (Columbia University)</p>	<p>Android</p> <p>ProcHarvester: Fully Automated Analysis of Procs Side-Channel Leaks on Android Raphael Spreitzer, Felix Kirchengast, Daniel Gruss, and Stefan Mangard (Graz University of Technology)</p> <p>Droid M+: Developer Support for Imbibing Android's New Permission Model Ioannis Gasparis, Azeem Aqil, Zhiyun Qian, Chengyu Song, Srikanth V. Krishnamurthy, Rajiv Gupta (University of California, Riverside); and Edward Colbert (U.S. Army Research Lab)</p> <p>Dazed Droids: A Longitudinal Study of Android Inter-App Vulnerabilities Ryan Johnson (Kryptowire / George Mason University); Mohamed Elsabagh (Kryptowire); Angelos Stavrou (Kryptowire / George Mason University); and Jeff Offutt (George Mason University)</p>	