

26TH USENIX SECURITY SYMPOSIUM



AUGUST 16–18, 2017 • VANCOUVER, BC, CANADA

Wednesday, August 16

7:30 am–9:00 am Continental Breakfast Grand Ballroom Foyer

9:00 am–9:30 am

Opening Remarks and Awards

Program Co-Chairs: Engin Kirda, *Northeastern University*, and Thomas Ristenpart, *Cornell Tech*

Grand Ballroom

9:30 am–10:30 am

Keynote Address

When Your Threat Model Is “Everything”: Defensive Security in Modern Newsrooms

Erinn Clark, *Lead Security Architect, First Look Media/The Intercept*

Grand Ballroom

10:30 am–11:00 am

Break with Refreshments

Grand Ballroom Foyer

11:00 am–12:30 pm

Track 1 Grand Ballroom AB

Bug Finding I

How Double-Fetch Situations turn into Double-Fetch Vulnerabilities: A Study of Double Fetches in the Linux Kernel

Pengfei Wang, *National University of Defense Technology*; Jens Krinke, *University College London*; Kai Lu and Gen Li, *National University of Defense Technology*; Steve Dodier-Lazaro, *University College London*

Postmortem Program Analysis with Hardware-Enhanced Post-Crash Artifacts

Jun Xu, Dongliang Mu, Xinyu Xing, Peng Liu, and Ping Chen, *The Pennsylvania State University*; Bing Mao, *Nanjing University*

Ninja: Towards Transparent Tracing and Debugging on ARM

Zhenyu Ning and Fengwei Zhang, *Wayne State University*

Track 2 Grand Ballroom CD

Side-Channel Attacks I

Prime+Abort: A Timer-Free High-Precision L3 Cache Attack using Intel TSX

Craig Disselkoen, David Kohlbrenner, Leo Porter, and Dean Tullsen, *University of California, San Diego*

On the effectiveness of mitigations against floating-point timing channels

David Kohlbrenner and Hovav Shacham, *UC San Diego*

Constant-Time Callees with Variable-Time Callers

Cesar Pereida García and Billy Bob Brumley, *Tampere University of Technology*

Track 3 Junior Ballroom

Systems Security I

Neural Nets Can Learn Function Type Signatures From Binaries

Zheng Leong Chua, Shiqi Shen, Prateek Saxena, and Zhenkai Liang, *National University of Singapore*

CAN't Touch This: Software-only Mitigation against Rowhammer Attacks targeting Kernel Memory

Ferdinand Brasser, *Technische Universität Darmstadt*; Lucas Davi, *University of Duisburg-Essen*; David Gens, Christopher Liebchen, and Ahmad-Reza Sadeghi, *Technische Universität Darmstadt*

Efficient Protection of Path-Sensitive Control Security

Ren Ding and Chenxiong Qian, *Georgia Tech*; Chengyu Song, *UC Riverside*; Bill Harris, Taesoo Kim, and Wenke Lee, *Georgia Tech*

12:30 pm–2:00 pm

Lunch (on your own)

2:00 pm–3:30 pm

Bug Finding II

Digtool: A Virtualization-Based Framework for Detecting Windows Kernel-Level Vulnerabilities

Jianfeng Pan, Guanglu Yan, and Xiaocao Fan, *IceSword Lab, 360 Internet Security Center*

kAFL: Hardware-Assisted Feedback Fuzzing for OS Kernels

Sergej Schumilo, Cornelius Aschermann, and Robert Gawlik, *Ruhr-Universität Bochum*; Sebastian Schinzel, *Münster University of Applied Sciences*; Thorsten Holz, *Ruhr-Universität Bochum*

Venerable Variadic Vulnerabilities Vanquished

Priyam Biswas, *Purdue University*; Alessandro Di Federico, *Politecnico di Milano*; Scott A. Carr, *Purdue University*; Prabhu Rajasekaran, Stijn Volckaert, Yeoul Na, and Michael Franz, *University of California, Irvine*; Mathias Payer, *Purdue University*

Side-Channel Countermeasures

Towards Practical Tools for Side Channel Aware Software Engineering: ‘Grey Box’ Modelling For Instruction Leakages

David McCann, Carolyn Whitnall, and Elisabeth Oswald, *University of Bristol*

Strong and Efficient Cache Side-Channel Protection using Hardware Transactional Memory

Daniel Gruss, *Graz University of Technology, Graz, Austria*; Felix Schuster, Olya Ohrimenko, and Istvan Haller, *Microsoft Research, Cambridge, UK*; Julian Lettner, *University of California, Irvine, USA*; Manuel Costa, *Microsoft Research, Cambridge, UK*

CacheD: Identifying Cache-Based Timing Channels in Production Software

Shuai Wang, Pei Wang, Xiao Liu, Danfeng Zhang, and Dinghao Wu, *The Pennsylvania State University*

Invited Talks

Title TBA

Ellen Cram Kowalczyk, *Microsoft*

From Problems to Patterns to Practice: Privacy and User Respect in a Complex World

Lea Kissner, *Product Privacy Lead and Principal Engineer, Google*

Wednesday, August 16 (continued)

3:30 pm–4:00 pm

Break with Refreshments

Grand Ballroom Foyer

4:00 pm–5:30 pm

Track 1 Grand Ballroom AB

Malware and Binary Analysis

BinSim: Trace-based Semantic Binary Diffing via System Call Sliced Segment Equivalence Checking

Jiang Ming, *University of Texas at Arlington*; Dongpeng Xu, Yufei Jiang, and Dinghao Wu, *Pennsylvania State University*

PlatPal: Detecting Malicious Documents with Platform Diversity

Meng Xu and Taesoo Kim, *Georgia Institute of Technology*

Malton: Towards On-Device Non-Invasive Mobile Malware Analysis for ART

Lei Xue, *The Hong Kong Polytechnic University*; Yajin Zhou, *unaffiliated*; Ting Chen, *University of Electronic Science and Technology of China*; Xiapu Luo, *The Hong Kong Polytechnic University*; Guofei Gu, *Texas A&M University*

Track 2 Grand Ballroom CD

Censorship

Global Measurement of DNS Censorship

Paul Pearce, *UC Berkeley*; Ben Jones, *Princeton*; Frank Li, *UC Berkeley*; Roya Ensafi and Nick Feamster, *Princeton*; Nick Weaver, *ICS*; Vern Paxson, *UC Berkeley*

Characterizing the Nature and Dynamics of Tor Exit Blocking

Rachee Singh, *University of Massachusetts–Amherst*; Rishab Nithyanand, *Stony Brook University*; Sadia Afroz, *University of California, Berkeley and International Computer Science Institute*; Paul Pearce, *UC Berkeley*; Michael Carl Tschantz, *International Computer Science Institute*; Phillipa Gill, *University of Massachusetts–Amherst*; Vern Paxson, *University of California, Berkeley and International Computer Science Institute*

DeTor: Provably Avoiding Geographic Regions in Tor

Zhihao Li, Stephen Herwig, and Dave Levin, *University of Maryland*

Track 3 Junior Ballroom

Embedded Systems

SmartAuth: User-Centered Authorization for the Internet of Things

Yuan Tian, *Carnegie Mellon University*; Nan Zhang, *Indiana University, Bloomington*; Yueh-Hsun Lin, *Samsung*; Xiaofeng Wang, *Indiana University, Bloomington*; Blase Ur, *University of Chicago*; Xianzheng Guo and Patrick Tague, *Carnegie Mellon University*

Aware: Preventing Abuse of Privacy-Sensitive Sensors via Operation Bindings

Giuseppe Petracca, *The Pennsylvania State University, US*; Ahmad-Atamli Reineh, *University of Oxford, UK*; Yuqiong Sun, *Symantec Research Labs*; Jens Grossklags, *Technical University of Munich, DE*; Trent Jaeger, *The Pennsylvania State University, US*

6thSense: A Context-aware Sensor-based Attack Detector for Smart Devices

Amit Kumar Sikder, Hidayet Aksu, and A. Selcuk Uluagac, *Florida International University*

6:00 pm–7:30 pm

Symposium Reception

Don't miss the USENIX Security '17 Reception, featuring, dinner, drinks, and the chance to connect with other attendees, speakers, and conference organizers.

Fountain Square

8:30 pm–9:30 pm

Lightning Talks

This is intended as an informal session for short and engaging presentations on recent unpublished results, work in progress, or other topics of interest to the USENIX Security attendees. As in the past, talks do not always need to be serious and funny talks are encouraged! This year, USENIX will generously sponsor awards for the most engaging talks. Bragging rights and small cash prizes can be yours for a great talk! For full consideration, submit your lightning talk at <https://sec17lightning.usenix.hotcrp.com> through July 28, 2017. Only talks submitted by this deadline will be considered for the awards. You can continue submitting talks through HotCRP or by emailing sec17lightning@usenix.org until Wednesday, August 16, 2017, 12:00 pm PDT.

Junior Ballroom

Thursday, August 17

8:00 am–9:00 am	Continental Breakfast	Grand Ballroom Foyer
9:00 am–10:30 am		

Track 1 Grand Ballroom AB

Networking Security

Identifier Binding Attacks and Defenses in Software-Defined Networks

Samuel Jero, *Purdue University*; William Koch, *Boston University*; Richard Skowyra and Hamed Okhravi, *MIT Lincoln Laboratory*; Cristina Nita-Rotaru, *Northeastern University*; David Bigelow, *MIT Lincoln Laboratory*

HELP: Helper-Enabled In-Band Device Pairing Resistant Against Signal Cancellation

Nirnimesh Ghose, Loukas Lazos, and Ming Li, *Electrical and Computer Engineering, University of Arizona, Tucson, AZ*

Attacking the Brain: Races in the SDN Control Plane

Lei Xu, Jeff Huang, Sungmin Hong, Jialong Zhang, and Guofei Gu, *Texas A&M University*

Track 2 Grand Ballroom CD

Targeted Attacks

Detecting Credential Spearphishing in Enterprise Settings

Grant Ho, *UC Berkeley*; Aashish Sharma, *The Lawrence Berkeley National Laboratory*; Mobin Javed, *UC Berkeley*; Vern Paxson, *UC Berkeley and ICSI*; David Wagner, *UC Berkeley*

SLEUTH: Real-time Attack Scenario Reconstruction from COTS Audit Data

Md Nahid Hossain, *Stony Brook University*; Sadeq M. Milajerdi, *University of Illinois at Chicago*; Junao Wang, *Stony Brook University*; Birhanu Eshete and Rigel Gjomemo, *University of Illinois at Chicago*; R. Sekar and Scott Stoller, *Stony Brook University*; V.N. Venkatakrishnan, *University of Illinois at Chicago*

When the Weakest Link is Strong: Secure Collaboration in the Case of the Panama Papers

Susan E. McGregor, *Columbia Journalism School*; Elizabeth Anne Watkins, *Columbia University*; Mahdi Nasrullah Al-Ameen and Kelly Caine, *Clemson University*; Franziska Roesner, *University of Washington*

Track 3 Junior Ballroom

Trusted Hardware

Hacking in Darkness: Return-oriented Programming against Secure Enclaves

Jaehyuk Lee and Jinsoo Jang, *KAIST*; Yeongjin Jang, *Georgia Institute of Technology*; Nohyun Kwak, Yeseul Choi, and Changho Choi, *KAIST*; Taesoo Kim, *Georgia Institute of Technology*; Marcus Peinado, *Microsoft Research*; Brent Byunghoon Kang, *KAIST*

vTZ: Virtualizing ARM TrustZone

Zhichao Hua, Jinyu Gu, Yubin Xia, Haibo Chen, Binyu Zang, and Haibing Guan, *Shanghai Key Laboratory of Scalable Computing and Systems, Shanghai Jiao Tong University*

Inferring Fine-grained Control Flow Inside SGX Enclaves with Branch Shadowing

Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, and Hyesoon Kim, *Georgia Institute of Technology*; Marcus Peinado, *Microsoft Research*

10:30 am–11:00 am	Break with Refreshments	Grand Ballroom Foyer
11:00 am–12:30 pm		

Authentication

AuthentiCall: Efficient Identity and Content Authentication for Phone Calls

Bradley Reaves, Logan Blue, Hadi Abdullah, Luis Vargas, Patrick Traynor, and Thomas Shrimpton, *University of Florida*

Picking Up My Tab: Understanding and Mitigating Synchronized Token Lifting and Spending in Mobile Payment

Xiaolong Bai, *Tsinghua University*; Zhe Zhou, *The Chinese University of Hong Kong*; XiaoFeng Wang, *Indiana University Bloomington*; Zhou Li, *IEEE Member*; Xianghang Mi and Nan Zhang, *Indiana University Bloomington*; Tongxin Li, *Peking University*; Shi-Min Hu, *Tsinghua University*; Kehuan Zhang, *The Chinese University of Hong Kong*

TrustBase: An Architecture to Repair and Strengthen Certificate-based Authentication

Mark O'Neill, Scott Heidbrink, Scott Ruoti, Jordan Whitehead, Dan Bunker, Luke Dickinson, Travis Hendershot, Joshua Reynolds, Kent Seamons, and Daniel Zappala, *Brigham Young University*

Malware and Obfuscation

Transcend: Detecting Concept Drift in Malware Classification Models

Roberto Jordaney and Kumar Sharad, *Royal Holloway, University of London*; Santanu K. Dash, *University College London*; Zhi Wang, Davide Papini, Ilija Nouretdinov, and Lorenzo Cavallaro, *Royal Holloway, University of London*

Syntia: Synthesizing the Semantics of Obfuscated Code

Tim Blazytko, Moritz Contag, Cornelius Aschermann, and Thorsten Holz, *Ruhr-Universität Bochum*

Predicting the Resilience of Obfuscated Code Against Symbolic Execution Attacks via Machine Learning

Sebastian Banescu, *Technische Universität München*; Christian Collberg, *University of Arizona*; Alexander Pretschner, *Technische Universität München*

Invited Talks

Title TBA

Abhradeep Guha Thakurta, *Assistant Professor, University of California, Santa Cruz*

OSS-Fuzz - Google's continuous fuzzing service for open source software

Kostya Serebryany, *Google*

12:30 pm–2:00 pm	Symposium Luncheon <i>Sponsored by Facebook</i>	Pavilion Ballroom
------------------	--	-------------------

The Internet Defense Prize will be presented at the Symposium Luncheon.

Thursday, August 17 (continued)

2:00 pm–3:30 pm

Track 1 Grand Ballroom AB

Web Security I

Extension Breakdown: Security Analysis of Browsers Extension Resources Control Policies

Iskander Sanchez-Rola and Igor Santos, *DeustoTech, University of Deusto*; Davide Balzarotti, *Eurecom*

CCSP: Controlled Relaxation of Content Security Policies by Runtime Policy Composition

Stefano Calzavara, Alvise Rabitti, and Michele Bugliesi, *Università Ca' Foscari Venezia*

Same-Origin Policy: Evaluation in Modern Browsers

Jörg Schwenk, Marcus Niemiets, and Christian Mainka, *Horst Görtz Institute for IT Security, Chair for Network and Data Security, Ruhr-University Bochum*

Track 2 Grand Ballroom CD

Privacy

Locally Differentially Private Protocols for Frequency Estimation

Tianhao Wang, Jeremiah Blocki, and Ninghui Li, *Purdue University*; Somesh Jha, *University of Wisconsin Madison*

BLENDER: Enabling Local Search with a Hybrid Differential Privacy Model

Brendan Avent and Aleksandra Korolova, *University of Southern California*; David Zeber and Torgeir Hovden, *Mozilla*; Benjamin Livshits, *Imperial College London*

Computer Security, Privacy, and DNA Sequencing

Peter Ney, Karl Koscher, Lee Organick, Luis Ceze, and Tadayoshi Kohno, *University of Washington*

Track 3 Junior Ballroom

Systems Security II

BootStomp: On the Security of Bootloaders in Mobile Devices

Nilo Redini, Aravind Machiry, Dipanjan Das, Yanick Fratantonio, Antonio Bianchi, Eric Gustafson, Yan Shoshitaishvili, Christopher Kruegel, and Giovanni Vigna, *UC Santa Barbara*

Seeing Through The Same Lens: Introspecting Guest Address Space At Native Speed

Siqi Zhao and Xuhua Ding, *Singapore Management University*; Wen Xu, *Georgia Institute of Technology*; Dawu Gu, *Shanghai JiaoTong University*

Oscar: A Practical Page-Permissions-Based Scheme for Thwarting Dangling Pointers

Thurston H.Y. Dang, *University of California, Berkeley*; Petros Maniatis, *Google Brain*; David Wagner, *University of California, Berkeley*

3:30 pm–4:00 pm

Break with Refreshments

Grand Ballroom Foyer

4:00 pm–5:30 pm

Web Security II

PDF Mirage: Content Masking Attack Against Information-Based Online Services

Ian Markwood, Dakun Shen, Yao Liu, and Zhuo Lu, *University of South Florida*

Loophole: Timing Attacks on Shared Event Loops in Chrome

Pepe Vila and Boris Köpf, *IMDEA Software Institute*

Game of Registrars: An Empirical Analysis of Post-Expiration Domain Name Takeovers

Tobias Lauinger, *Northeastern University*; Abdelberi Chaabane, *unaffiliated*; Ahmet Salih Buyukkayhan, *Northeastern University*; Kaan Onarlioglu, *unaffiliated*; Wil Robertson, *Northeastern University*

Applied Cryptography

Speeding up detection of SHA-1 collision attacks using unavoidable attack conditions

Marc Stevens, *CWI*; Daniel Shumow, *Microsoft Research*

Pheonix: Rebirth of a Cryptographic Password-Hardening Service

Russell W. F. Lai, *Chinese University of Hong Kong*; Christoph Egger and Dominique Schröder, *Friedrich-Alexander-University*; Sherman S. M. Chow, *Chinese University of Hong Kong*

Vale: Verifying High-Performance Cryptographic Assembly Code

Barry Bond and Chris Hawblitzel, *Microsoft Research*; Manos Kapritsos, *University of Michigan*; K. Rustan M. Leino and Jacob R. Lorch, *Microsoft Research*; Bryan Parno, *Carnegie Mellon University*; Ashay Rane, *University of Texas*; Srinath Setty, *Microsoft Research*; Laure Thompson, *Cornell University*

Invited Talks

DDoS Panel

Moderator: Michael Bailey, *University of Illinois, at Urbana-Champaign*

6:00 pm–7:30 pm

Poster Session and Happy Hour

Pavilion Ballroom and Foyer

Check out the cool new ideas and the latest preliminary research on display at the Poster Session and Happy Hour. Take part in discussions with your colleagues over complimentary drinks and snacks. View the list of accepted posters at www.usenix.org/usenixsecurity17/posters.

7:30 pm–9:30 pm

USENIX Security '17 Doctoral Colloquium

Junior Ballroom

What opportunities await security students graduating with a PhD? On Thursday evening, students will have the opportunity to listen to informal panels of faculty and industrial researchers providing personal perspectives on their post-PhD career search. Learn about the academic job search, the industrial research job search, research fund raising, dual-career challenges, life uncertainty, and other idiosyncrasies of the ivory tower. The event is organized by Thorsten Holz. If you would like to speak in the Doctoral Colloquium, please email sec17dc@usenix.org.

Friday, August 18

8:00 am–9:00 am Continental Breakfast Grand Ballroom Foyer

9:00 am–10:30 am

Track 1 Grand Ballroom AB

Web Security III

Exploring User Perceptions of Discrimination in Online Targeted Advertising

Angelisa C. Plane, Elissa M. Redmiles, and Michelle L. Mazurek, *University of Maryland College Park*; Michael Carl Tschantz, *International Computer Science Institute*

Measuring the Insecurity of Mobile Deep Links of Android

Fang Liu, Chun Wang, Andres Chavez, Danfeng Yao, and Gang Wang, *Virginia Tech*

How the Web Tangled Itself: Uncovering the History of Client-Side Web (In)Security

Ben Stock, *CISPA, Saarland University*; Martin Johns, *SAP SE*; Marius Steffens and Michael Backes, *CISPA, Saarland University*

Track 2 Grand Ballroom CD

Software Security

Towards Efficient Heap Overflow Discovery

Xiangkun Jia, *TCA/SK LCS, Institute of Software, Chinese Academy of Sciences*; Chao Zhang, *Institute for Network Science and Cyberspace, Tsinghua University*; Purui Su, Yi Yang, Huafeng Huang, and Dengguo Feng, *TCA/SK LCS, Institute of Software, Chinese Academy of Sciences*

DR. CHECKER: A Soundy Analysis for Linux Kernel Drivers

Aravind Machiry, Chad Spensky, Jacob Corina, Nick Stephens, Christopher Kruegel, and Giovanni Vigna, *UC Santa Barbara*

Dead Store Elimination (Still) Considered Harmful

Zhaomo Yang and Brian Johannsmeyer, *University of California, San Diego*; Anders Trier Olesen, *Aalborg University*; Sorin Lerner and Kirill Levchenko, *University of California, San Diego*

Track 3 Junior Ballroom

Side-Channel Attacks II

Telling Your Secrets without Page Faults: Stealthy Page Table-Based Attacks on Enclaved Execution

Jo Van Bulck, *KU Leuven*; Nico Weichbrodt and Rüdiger Kapitza, *TU Braunschweig*; Frank Piessens and Raoul Strackx, *KU Leuven*

CLKSCREW: Exposing the Perils of Security-Oblivious Energy Management

Adrian Tang, Simha Sethumadhavan, and Salvatore Stolfo, *Columbia University*

AutoLock: Why Cache Attacks on ARM Are Harder Than You Think

Marc Green, *Worcester Polytechnic Institute*; Leandro Rodrigues and Andreas Zankl, *Fraunhofer AISEC*; Gorka Irazoqui, *Worcester Polytechnic Institute*; Johann Heyszl, *Fraunhofer AISEC*; Thomas Eisenbarth, *Worcester Polytechnic Institute*

10:30 am–11:00 am Break with Refreshments Grand Ballroom Foyer

11:00 am–12:30 pm

Understanding Attacks

Understanding the Mirai Botnet

Manos Antonakakis, *Georgia Institute of Technology*; Tim April, *Akamai*; Michael Bailey, *University of Illinois, Urbana-Champaign*; Matt Bernhard, *University of Michigan, Ann Arbor*; Elie Bursztein, *Google*; Jaime Cochran, *Cloudflare*; Zakir Durumeric and J. Alex Halderman, *University of Michigan, Ann Arbor*; Luca Invernizzi, *Google*; Michalis Kallitsis, *Merit Network, Inc.*; Deepak Kumar, *University of Illinois, Urbana-Champaign*; Chaz Lever, *Georgia Institute of Technology*; Zane Ma, *University of Illinois, Urbana-Champaign*; Joshua Mason, *University of Illinois, Urbana-Champaign*; Damian Menscher, *Google*; Chad Seaman, *Akamai*; Nick Sullivan, *Cloudflare*; Kurt Thomas, *Google*; Yi Zhou, *University of Illinois, Urbana-Champaign*

MPI: Multiple Perspective Attack Investigation with Semantic Aware Execution Partitioning

Shiqing Ma, *Purdue University*; Juan Zhai, *Nanjing University*; Fei Wang, *Purdue University*; Kyu Hyung Lee, *University of Georgia*; Xiangyu Zhang and Dongyan Xu, *Purdue University*

Detecting Android Root Exploits by Learning from Root Providers

Ioannis Gasparis, Zhiyun Qian, Chengyu Song, and Srikanth V. Krishnamurthy, *University of California, Riverside*

Hardware Security

USB Snooping Made Easy: Crosstalk Leakage Attacks on USB Hubs

Yang Su, *The University of Adelaide*; Daniel Genkin, *University of Pennsylvania and University of Maryland*; Damith Ranasinghe, *The University of Adelaide*; Yuval Yarom, *The University of Adelaide and Data61, CSIRO*

Reverse Engineering x86 Processor Microcode

Philipp Koppe, Benjamin Kollenda, Marc Fyrbiak, Christian Kison, Robert Gawlik, Christof Paar, and Thorsten Holz, *Ruhr-University Bochum*

See No Evil, Hear No Evil, Feel No Evil, Print No Evil? Malicious Fill Patterns Detection in Additive Manufacturing

Christian Bayens, *Georgia Institute of Technology*; Tuan Le and Luis Garcia, *Rutgers University*; Raheem Beyah, *Georgia Institute of Technology*; Mehdi Javanmard and Saman Zonouz, *Rutgers University*

Privacy & Anonymity Systems

The Loopix Anonymity System

Ania Piotrowska and Jamie Hayes, *University College London*; Tariq Elahi, *KU Leuven*; Sebastian Meiser and George Danezis, *University College London*

MCMix: Anonymous Messaging via Secure Multiparty Computation

Nikolaos Alexopoulos, *TU Darmstadt*; Aggelos Kiayias, *University of Edinburgh*; Riivo Talviste, *Cybernetica AS*; Thomas Zacharias, *University of Edinburgh*

ORide: A Privacy-Preserving yet Accountable Ride-Hailing Service

Anh Pham, Italo Dacosta, Guillaume Endignoux, and Juan Ramon Troncoso Pastoriza, *EPFL*; Kevin Huguenin, *UNIL*; Jean-Pierre Hubaux, *EPFL*

12:30 pm–2:00 pm Lunch (on your own)

Friday, August 18 (continued)

2:00 pm–3:30 pm

Track 1 Grand Ballroom AB

Software Integrity

Adaptive Android Kernel Live Patching

Yue Chen, *Florida State University*; Yulong Zhang, *Baidu X-Lab*; Zhi Wang, *Florida State University*; Liangzhao Xia, Chenfu Bao, and Tao Wei, *Baidu X-Lab*

CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds

Kirill Nikitin, Lefteris Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, and Linus Gasser, *EPFL*; Ismail Khoffi, *University of Bonn*; Justin Cappos, *New York University*; Bryan Ford, *EPFL*

ROTE: Rollback Protection for Trusted Execution

Sinisa Matetic, Mansoor Ahmed, Kari Kostianinen, Aritra Dhar, David Sommer, and Arthur Gervais, *ETH Zurich*; Ari Juels, *Cornell Tech*; Srdjan Capkun, *ETH Zurich*

Track 2 Grand Ballroom CD

Crypto Deployment

A Longitudinal, End-to-End View of the DNSSEC Ecosystem

Taejoong Chung, *Northeastern University*; Roland van Rijswijk-Deij, *University of Twente and SURFnet bv*; Balakrishnan Chandrasekaran, *TU Berlin*; David Choffnes, *Northeastern University*; Dave Levin, *University of Maryland*; Bruce M. Maggs, *Duke University and Akamai Technologies*; Alan Mislove and Christo Wilson, *Northeastern University*

Measuring HTTPS Adoption on the Web

Adrienne Porter Felt, *Google*; Richard Barnes and April King, *Mozilla*; Chris Palmer and Chris Bentzel, *Google*

"I Have No Idea What I'm Doing"—On the Usability of Deploying HTTPS

Katharina Krombholz, Wilfried Mayer, Martin Schmiedecker, and Edgar Weippl, *SBA Research*

Track 3 Junior Ballroom

Privacy Attacks & Defense

Beauty and the Burst: Remote Identification of Encrypted Video Streams

Roei Schuster, *Tel Aviv University, Cornell-Tech*; Vitaly Shmatikov, *Cornell-Tech*; Eran Tromer, *Tel Aviv University, Columbia University*

Walkie-Talkie: An Efficient Defense Against Passive Website Fingerprinting Attacks

Tao Wang, *Hong Kong University of Science and Technology*; Ian Goldberg, *University of Waterloo*

A Privacy Analysis of Cross-device Tracking

Sebastian Zimmeck, *Carnegie Mellon University*; Jie S. Li and Hyungtae Kim, *unaffiliated*; Steven M. Bellovin and Tony Jebara, *Columbia University*

3:30 pm–4:00 pm

Break with Refreshments

Grand Ballroom Foyer

4:00 pm–5:30 pm

Blockchains

SmartPool: Practical Decentralized Pooled Mining

Loi Luu, *National University of Singapore*; Yaron Velner, *The Hebrew University of Jerusalem*; Jason Teutsch, *TrueBit Foundation*; Prateek Saxena, *National University of Singapore*

REM: Resource-Efficient Mining for Blockchains

Fan Zhang, Ittay Eyal, and Robert Escriva, *Cornell University*; Ari Juels, *Cornell Tech*; Robbert van Renesse, *Cornell University*

Databases

Ensuring Authorized Updates in Multi-user Database-Backed Applications

Kevin Eykholt, Atul Prakash, and Barzan Mozafari, *University of Michigan Ann Arbor*

Qapla: Policy compliance for database-backed systems

Aastha Mehta and Eslam Elnikety, *MPI-SWS*; Katura Harvey, *University of Maryland, College Park*; Deepak Garg and Peter Druschel, *MPI-SWS*

Invited Talks

Data Hemorrhage, Inequality, and You: How Technology and Data Flows are Changing the Civil Liberties Game

Shankar Narayan, *Technology and Liberty Project Director, American Civil Liberties Union of Washington*