

28th USENIX Security Symposium (USENIX Security'19)

Santa Clara, California, USA
14 - 16 August 2019

Volume 1 of 3

ISBN: 978-1-7138-0410-9

Printed from e-media with permission by:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571



Some format issues inherent in the e-media version may also appear in this print version.

Copyright© (2019) by Usenix Association
All rights reserved.

Printed with permission by Curran Associates, Inc. (2020)

For permission requests, please contact Usenix Association
at the address below.

Usenix Association
2560 Ninth Street, Suite 215
Berkeley, California, 94710

<https://www.usenix.org/>

Additional copies of this publication are available from:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: 845-758-0400
Fax: 845-758-2633
Email: curran@proceedings.com
Web: www.proceedings.com

USENIX Security '19:
28th USENIX Security Symposium
August 14–16, 2019
Santa Clara, CA, USA

Wireless Security

A Study of the Feasibility of Co-located App Attacks against BLE and a Large-Scale Analysis of the Current Application-Layer Security Landscape 1
Pallavi Sivakumaran and Jorge Blasco, *Royal Holloway University of London*

The CrossPath Attack: Disrupting the SDN Control Channel via Shared Links 19
Jiahao Cao, Qi Li, and Renjie Xie, *Tsinghua University*; Kun Sun, *George Mason University*; Guofei Gu, *Texas A&M University*; Mingwei Xu and Yuan Yang, *Tsinghua University*

A Billion Open Interfaces for Eve and Mallory: MitM, DoS, and Tracking Attacks on iOS and macOS Through Apple Wireless Direct Link 37
Milan Stute, *Technische Universität Darmstadt*; Sashank Narain, *Northeastern University*; Alex Mariotto, Alexander Heinrich, and David Kreitschmann, *Technische Universität Darmstadt*; Guevara Noubir, *Northeastern University*; Matthias Hollick, *Technische Universität Darmstadt*

Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE 55
Hojoon Yang, Sangwook Bae, Mincheol Son, Hongil Kim, Song Min Kim, and Yongdae Kim, *KAIST*

UWB-ED: Distance Enlargement Attack Detection in Ultra-Wideband 73
Mridula Singh, Patrick Leu, AbdelRahman Abdou, and Srdjan Capkun, *ETH Zurich*

Protecting Users Everywhere

Computer Security and Privacy in the Interactions Between Victim Service Providers and Human Trafficking Survivors 89
Christine Chen, *University of Washington*; Nicola Dell, *Cornell Tech*; Franziska Roesner, *University of Washington*

Clinical Computer Security for Victims of Intimate Partner Violence 105
Sam Havron, Diana Freed, and Rahul Chatterjee, *Cornell Tech*; Damon McCoy, *New York University*; Nicola Dell and Thomas Ristenpart, *Cornell Tech*

Evaluating the Contextual Integrity of Privacy Regulation: Parents' IoT Toy Privacy Norms Versus COPPA 123
Noah Athorpe, Sarah Varghese, and Nick Feamster, *Princeton University*

Secure Multi-User Content Sharing for Augmented Reality Applications 141
Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner, *University of Washington*

Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study 159
Eric Zeng and Franziska Roesner, *University of Washington*

Hardware Security

PAC it up: Towards Pointer Integrity using ARM Pointer Authentication 177
Hans Liljestrand, *Aalto University, Huawei Technologies Oy*; Thomas Nyman, *Aalto University*; Kui Wang, *Huawei Technologies Oy, Tampere University of Technology*; Carlos China Perez, *Huawei Technologies Oy*; Jan-Erik Ekberg, *Huawei Technologies Oy, Aalto University*; N. Asokan, *Aalto University*

Origin-sensitive Control Flow Integrity 195
Mustakimur Rahman Khandaker, Wenqing Liu, Abu Naser, Zhi Wang, and Jie Yang, *Florida State University*

(continued on next page)

HardFails: Insights into Software-Exploitable Hardware Bugs	213
Ghada Dessouky and David Gens, <i>Technische Universität Darmstadt</i> ; Patrick Haney and Garrett Persyn, <i>Texas A&M University</i> ; Arun Kanuparthi, Hareesh Khattri, and Jason M. Fung, <i>Intel Corporation</i> ; Ahmad-Reza Sadeghi, <i>Technische Universität Darmstadt</i> ; Jeyavijayan Rajendran, <i>Texas A&M University</i>	
uXOM: Efficient eXecute-Only Memory on ARM Cortex-M	231
Donghyun Kwon, Jangseop Shin, and Giyeol Kim, <i>Seoul National University</i> ; Byoungyoung Lee, <i>Seoul National University, Purdue University</i> ; Yeongpil Cho, <i>Soongsil University</i> ; Yunheung Paek, <i>Seoul National University</i>	
A Systematic Evaluation of Transient Execution Attacks and Defenses	249
Claudio Canella, <i>Graz University of Technology</i> ; Jo Van Bulck, <i>imec-DistriNet, KU Leuven</i> ; Michael Schwarz, Moritz Lipp, Benjamin von Berg, and Philipp Ortner, <i>Graz University of Technology</i> ; Frank Piessens, <i>imec-DistriNet, KU Leuven</i> ; Dmitry Evtushkin, <i>College of William and Mary</i> ; Daniel Gruss, <i>Graz University of Technology</i>	
Machine Learning Applications	
The Secret Sharer: Evaluating and Testing Unintended Memorization in Neural Networks	267
Nicholas Carlini, <i>Google Brain</i> ; Chang Liu, <i>University of California, Berkeley</i> ; Úlfar Erlingsson, <i>Google Brain</i> ; Jernej Kos, <i>National University of Singapore</i> ; Dawn Song, <i>University of California, Berkeley</i>	
Improving Robustness of ML Classifiers against Realizable Evasion Attacks Using Conserved Features	285
Liang Tong, <i>Washington University in St. Louis</i> ; Bo Li, <i>UIUC</i> ; Chen Hajaj, <i>Ariel University</i> ; Chaowei Xiao, <i>University of Michigan</i> ; Ning Zhang and Yevgeniy Vorobeychik, <i>Washington University in St. Louis</i>	
ALOHA: Auxiliary Loss Optimization for Hypothesis Augmentation	303
Ethan M. Rudd, Felipe N. Ducau, Cody Wild, Konstantin Berlin, and Richard Harang, <i>Sophos</i>	
Why Do Adversarial Attacks Transfer? Explaining Transferability of Evasion and Poisoning Attacks	321
Ambra Demontis, Marco Melis, and Maura Pintor, <i>University of Cagliari, Italy</i> ; Matthew Jagielski, <i>Northeastern University</i> ; Battista Biggio, <i>University of Cagliari, Italy, and Pluribus One</i> ; Alina Oprea and Cristina Nita-Rotaru, <i>Northeastern University</i> ; Fabio Roli, <i>University of Cagliari, Italy, and Pluribus One</i>	
Stack Overflow Considered Helpful! Deep Learning Security Nudges Towards Stronger Cryptography	339
Felix Fischer, <i>Technical University of Munich</i> ; Huang Xiao, <i>Bosch Center for Artificial Intelligence</i> ; Ching-Yu Kao, <i>Fraunhofer AISEC</i> ; Yannick Stachelscheid, Benjamin Johnson, and Danial Razar, <i>Technical University of Munich</i> ; Paul Fawkesley and Nat Buckley, <i>Projects by IF</i> ; Konstantin Böttinger, <i>Fraunhofer AISEC</i> ; Paul Muntean and Jens Grossklags, <i>Technical University of Munich</i>	
Planes, Cars, and Robots	
Wireless Attacks on Aircraft Instrument Landing Systems	357
Harshad Sathaye, Domien Schepers, Aanjhan Ranganathan, and Guevara Noubir, <i>Northeastern University</i>	
Please Pay Inside: Evaluating Bluetooth-based Detection of Gas Pump Skimmers	373
Nishant Bhaskar and Maxwell Bland, <i>University of California San Diego</i> ; Kirill Levchenko, <i>University of Illinois at Urbana-Champaign</i> ; Aaron Schulman, <i>University of California San Diego</i>	
CANvas: Fast and Inexpensive Automotive Network Mapping	389
Sekar Kulandaivel, Tushar Goyal, Arnav Kumar Agrawal, and Vyas Sekar, <i>Carnegie Mellon University</i>	
Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging	407
Richard Baker and Ivan Martinovic, <i>University of Oxford</i>	
RVFuzzer: Finding Input Validation Bugs in Robotic Vehicles through Control-Guided Testing	425
Taegyu Kim, <i>Purdue University</i> ; Chung Hwan Kim and Junghwan Rhee, <i>NEC Laboratories America</i> ; Fan Fei, Zhan Tu, Gregory Walkup, Xiangyu Zhang, Xinyan Deng, and Dongyan Xu, <i>Purdue University</i>	

Machine Learning, Adversarial and Otherwise

Seeing is Not Believing: Camouflage Attacks on Image Scaling Algorithms 443

Qixue Xiao, *Department of Computer Science and Technology, Tsinghua University and 360 Security Research Labs*; Yufei Chen, *School of Electronic and Information Engineering, Xi'an Jiaotong University and 360 Security Research Labs*; Chao Shen, *School of Electronic and Information Engineering, Xi'an Jiaotong University*; Yu Chen, *Department of Computer Science and Technology, Tsinghua University and Peng Cheng Laboratory*; Kang Li, *Department of Computer Science, University of Georgia*

CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning 461

Yisroel Mirsky and Tom Mahler, *Ben-Gurion University*; Ilan Shelef, *Soroka University Medical Center*; Yuval Elovici, *Ben-Gurion University*

Misleading Authorship Attribution of Source Code using Adversarial Learning 479

Erwin Quiring, Alwin Maier, and Konrad Rieck, *TU Braunschweig*

Terminal Brain Damage: Exposing the Graceless Degradation in Deep Neural Networks Under Hardware Fault Attacks 497

Sanghyun Hong, *University of Maryland College Park*; Pietro Frigo, *Vrije Universiteit Amsterdam*; Yiğitcan Kaya, *University of Maryland College Park*; Cristiano Giuffrida, *Vrije Universiteit Amsterdam*; Tudor Dumitraş, *University of Maryland College Park*

CSI NN: Reverse Engineering of Neural Network Architectures Through Electromagnetic Side Channel 515

Lejla Batina, *Radboud University, The Netherlands*; Shivam Bhasin and Dirmanto Jap, *Nanyang Technological University, Singapore*; Stjepan Picek, *Delft University of Technology, The Netherlands*

Mobile Security 1

simTPM: User-centric TPM for Mobile Devices 533

Dhiman Chakraborty, *CISPA Helmholtz Center for Information Security, Saarland University*; Lucjan Hanzlik, *CISPA Helmholtz Center for Information Security, Stanford University*; Sven Bugiel, *CISPA Helmholtz Center for Information Security*

The Betrayal At Cloud City: An Empirical Analysis Of Cloud-Based Mobile Backends 551

Omar Alrawi, *Georgia Institute of Technology*; Chaoshun Zuo, *Ohio State University*; Ruian Duan and Ranjita Pai Kasturi, *Georgia Institute of Technology*; Zhiqiang Lin, *Ohio State University*; Brendan Saltaformaggio, *Georgia Institute of Technology*

ENTrust: Regulating Sensor Access by Cooperating Programs via Delegation Graphs 567

Giuseppe Petracca, *Pennsylvania State University, US*; Yuqiong Sun, *Symantec Research Labs, US*; Ahmad-Atamli Reineh, *Alan Turing Institute, UK*; Patrick McDaniel, *Pennsylvania State University, US*; Jens Grossklags, *Technical University of Munich, DE*; Trent Jaeger, *Pennsylvania State University, US*

PolicyLint: Investigating Internal Privacy Policy Contradictions on Google Play 585

Benjamin Andow and Samin Yaseer Mahmud, *North Carolina State University*; Wenyu Wang, *University of Illinois at Urbana-Champaign*; Justin Whitaker, William Enck, and Bradley Reaves, *North Carolina State University*; Kapil Singh, *IBM T.J. Watson Research Center*; Tao Xie, *University of Illinois at Urbana-Champaign*

50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System 603

Joel Reardon, *University of Calgary / AppCensus Inc.*; Álvaro Feal, *IMDEA Networks Institute / Universidad Carlos III Madrid*; Primal Wijesekera, *U.C. Berkeley / ICSI*; Amit Elazari Bar On, *U.C. Berkeley*; Narseo Vallina-Rodriguez, *IMDEA Networks Institute / ICSI / AppCensus Inc.*; Serge Egelman, *U.C. Berkeley / ICSI / AppCensus Inc.*

Side Channels

SPOILER: Speculative Load Hazards Boost Rowhammer and Cache Attacks 621

Saad Islam and Ahmad Moghimi, *Worcester Polytechnic Institute*; Ida Bruhns and Moritz Krebbel, *University of Luebeck*; Berk Gulmezoglu, *Worcester Polytechnic Institute*; Thomas Eisenbarth, *Worcester Polytechnic Institute and University of Luebeck*; Berk Sunar, *Worcester Polytechnic Institute*

(continued on next page)

Robust Website Fingerprinting Through the Cache Occupancy Channel 639
Anatoly Shusterman, *Ben-Gurion University of the Negev*; Lachlan Kang, *University of Adelaide*; Yarden Haskal and Yosef Meltser, *Ben-Gurion University of the Negev*; Prateek Mittal, *Princeton University*; Yossi Oren, *Ben-Gurion University of the Negev*; Yuval Yarom, *University of Adelaide and Data61*

Identifying Cache-Based Side Channels through Secret-Augmented Abstract Interpretation 657
Shuai Wang, *HKUST*; Yuyan Bao and Xiao Liu, *Penn State University*; Pei Wang, *Baidu X-Lab*; Danfeng Zhang and Dinghao Wu, *Penn State University*

SCATTERCACHE: Thwarting Cache Attacks via Cache Set Randomization 675
Mario Werner, Thomas Unterluggauer, Lukas Giner, Michael Schwarz, Daniel Gruss, and Stefan Mangard, *Graz University of Technology*

Pythia: Remote Oracles for the Masses 693
Shin-Yeh Tsai, *Purdue University*; Mathias Payer, *EPFL*; Yiyang Zhang, *Purdue University*

Mobile Security 2

HideMyApp: Hiding the Presence of Sensitive Apps on Android 711
Anh Pham, *ABB Corporate Research*; Italo Dacosta, *EPFL*; Eleonora Losiouk, *University of Padova*; John Stephan, *EPFL*; Kévin Huguenin, *University of Lausanne*; Jean-Pierre Hubaux, *EPFL*

TESSERACT: Eliminating Experimental Bias in Malware Classification across Space and Time 729
Feargus Pendlebury, Fabio Pierazzi, and Roberto Jordaney, *King's College London & Royal Holloway, University of London*; Johannes Kinder, *Bundeswehr University Munich*; Lorenzo Cavallaro, *King's College London*

Devils in the Guidance: Predicting Logic Vulnerabilities in Payment Syndication Services through Automated Documentation Analysis. 747
Yi Chen, *Institute of Information Engineering, CAS*; Luyi Xing, Yue Qin, Xiaojing Liao, and XiaoFeng Wang, *Indiana University Bloomington*; Kai Chen and Wei Zou, *Institute of Information Engineering, CAS*

Understanding iOS-based Crowdturfing Through Hidden UI Analysis 765
Yeonjoon Lee, Xueqiang Wang, Kwangwuk Lee, Xiaojing Liao, and XiaoFeng Wang, *Indiana University*; Tongxin Li, *Peking University*; Xianghang Mi, *Indiana University*

Crypto Means Cryptocurrencies

BITE: Bitcoin Lightweight Client Privacy using Trusted Execution 783
Sinisa Matetic, Karl Wüst, Moritz Schneider, and Kari Kostianen, *ETH Zurich*; Ghassan Karame, *NEC Labs*; Srdjan Capkun, *ETH Zurich*

FASTKITTEN: Practical Smart Contracts on Bitcoin 801
Poulami Das, Lisa Eckey, Tommaso Frassetto, David Gens, Kristina Hostáková, Patrick Jauernig, Sebastian Faust, and Ahmad-Reza Sadeghi, *Technische Universität Darmstadt, Germany*

StrongChain: Transparent and Collaborative Proof-of-Work Consensus 819
Pawel Szalachowski, Daniël Reijtsbergen, and Ivan Homoliak, *Singapore University of Technology and Design (SUTD)*; Siwei Sun, *Institute of Information Engineering and DCS Center, Chinese Academy of Sciences*

Tracing Transactions Across Cryptocurrency Ledgers 837
Haaroon Yousaf, George Kappos, and Sarah Meiklejohn, *University College London*

Intelligence and Vulnerabilities

Reading the Tea leaves: A Comparative Analysis of Threat Intelligence 851
Vector Guo Li, *University of California, San Diego*; Matthew Dunn, *Northeastern University*; Paul Pearce, *Georgia Tech*; Damon McCoy, *New York University*; Geoffrey M. Voelker and Stefan Savage, *University of California, San Diego*; Kirill Levchenko, *University of Illinois Urbana-Champaign*

Towards the Detection of Inconsistencies in Public Security Vulnerability Reports 869
Ying Dong, *University of Chinese Academy of Sciences and The Pennsylvania State University*; Wenbo Guo, Yueqi Chen, and Xinyu Xing, *The Pennsylvania State University and JD Security Research Center*; Yuqing Zhang, *University of Chinese Academy of Sciences*; Gang Wang, *Virginia Tech*

Understanding and Securing Device Vulnerabilities through Automated Bug Report Analysis	887
<i>Xuan Feng, Beijing Key Laboratory of IOT Information Security Technology, Institute of Information Engineering, CAS, China; School of Cyber Security, University of Chinese Academy of Sciences, China; Xiaojing Liao and Xiaofeng Wang, Department of Computer Science, Indiana University Bloomington, USA; Haining Wang, Department of Electrical and Computer Engineering, University of Delaware, USA; Qiang Li, School of Computer and Information Technology, Beijing Jiaotong University, China; Kai Yang, Hongsong Zhu, and Limin Sun, Beijing Key Laboratory of IOT Information Security Technology, Institute of Information Engineering, CAS, China; School of Cyber Security, University of Chinese Academy of Sciences, China</i>	
ATTACK2VEC: Leveraging Temporal Word Embeddings to Understand the Evolution of Cyberattacks	905
<i>Yun Shen, Symantec Research Labs; Gianluca Stringhini, Boston University</i>	
Web Attacks	
Leaky Images: Targeted Privacy Attacks in the Web	923
<i>Cristian-Alexandru Staicu and Michael Pradel, TU Darmstadt</i>	
All Your Clicks Belong to Me: Investigating Click Interception on the Web	941
<i>Mingxue Zhang and Wei Meng, Chinese University of Hong Kong; Sangho Lee, Microsoft Research; Byoungyoung Lee, Seoul National University and Purdue University; Xinyu Xing, Pennsylvania State University</i>	
What Are You Searching For? A Remote Keylogging Attack on Search Engine Autocomplete	959
<i>John V. Monaco, Naval Postgraduate School</i>	
Iframes/Popups Are Dangerous in Mobile WebView: Studying and Mitigating Differential Context Vulnerabilities . .	977
<i>GuangLiang Yang, Jeff Huang, and Guofei Gu, Texas A&M University</i>	
Small World with High Risks: A Study of Security Threats in the npm Ecosystem	995
<i>Markus Zimmermann and Cristian-Alexandru Staicu, TU Darmstadt; Cam Tenny, r2c; Michael Pradel, TU Darmstadt</i>	
Crypto Means Cryptographic Attacks	
“Johnny, you are fired!” – Spoofing OpenPGP and S/MIME Signatures in Emails.	1011
<i>Jens Müller and Marcus Brinkmann, Ruhr University Bochum; Damian Poddebniak, Münster University of Applied Sciences; Hanno Böck, unaffiliated; Sebastian Schinzel, Münster University of Applied Sciences; Juraj Somorovsky and Jörg Schwenk, Ruhr University Bochum</i>	
Scalable Scanning and Automatic Classification of TLS Padding Oracle Vulnerabilities	1029
<i>Robert Merget and Juraj Somorovsky, Ruhr University Bochum; Nimrod Aviram, Tel Aviv University; Craig Young, Tripwire VERT; Janis Fliegenschmidt and Jörg Schwenk, Ruhr University Bochum; Yuval Shavitt, Tel Aviv University</i>	
The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation Of Bluetooth BR/EDR	1047
<i>Daniele Antonioli, SUTD; Nils Ole Tippenhauer, CISPA; Kasper B. Rasmussen, University of Oxford</i>	
From IP ID to Device ID and KASLR Bypass.	1063
<i>Amit Klein and Benny Pinkas, Bar Ilan University</i>	
When the Signal is in the Noise: Exploiting Diffix’s Sticky Noise	1081
<i>Andrea Gadotti and Florimond Houssiau, Imperial College London; Luc Rocher, Imperial College London and Université catholique de Louvain; Benjamin Livshits and Yves-Alexandre de Montjoye, Imperial College London</i>	
IoT Security	
FIRM-AFL: High-Throughput Greybox Fuzzing of IoT Firmware via Augmented Process Emulation	1099
<i>Yaowen Zheng, Beijing Key Laboratory of IOT Information Security Technology, Institute of Information Engineering, CAS, China; School of Cyber Security, University of Chinese Academy of Sciences, China; Ali Davanian, Heng Yin, and Chengyu Song, University of California, Riverside; Hongsong Zhu and Limin Sun, Beijing Key Laboratory of IOT Information Security Technology, Institute of Information Engineering, CAS, China; School of Cyber Security, University of Chinese Academy of Sciences, China</i>	

Not Everything is Dark and Gloomy: Power Grid Protections Against IoT Demand Attacks 1115
Bing Huang, *The University of Texas at Austin*; Alvaro A. Cardenas, *University of California, Santa Cruz*; Ross Baldick, *The University of Texas at Austin*

Discovering and Understanding the Security Hazards in the Interactions between IoT Devices, Mobile Apps, and Clouds on Smart Home Platforms. 1133
Wei Zhou, *National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences*;
Yan Jia, Yao Yao, and Lipeng Zhu, *School of Cyber Engineering, Xidian University*; *National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences*; Le Guan, *Department of Computer Science, University of Georgia*; Yuhang Mao, *School of Cyber Engineering, Xidian University*; *National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences*; Peng Liu, *College of Information Sciences and Technology, Pennsylvania State University*; Yuqing Zhang, *National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences*; *School of Cyber Engineering, Xidian University*; *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences*

Looking from the Mirror: Evaluating IoT Device Security through Mobile Companion Apps. 1151
Xueqiang Wang, *Indiana University Bloomington*; Yuqiong Sun and Susanta Nanda, *Symantec Research Labs*; XiaoFeng Wang, *Indiana University Bloomington*

All Things Considered: An Analysis of IoT Devices on Home Networks 1169
Deepak Kumar, *University of Illinois at Urbana-Champaign*; Kelly Shen and Benton Case, *Stanford University*; Deepali Garg, Galina Alperovich, Dmitry Kuznetsov, and Rajarshi Gupta, *Avast Software s.r.o.*; Zakir Durumeric, *Stanford University*

OS Security

KEPLER: Facilitating Control-flow Hijacking Primitive Evaluation for Linux Kernel Vulnerabilities 1187
Wei Wu, *Institute of Information Engineering, Chinese Academy of Sciences*; *Pennsylvania State University*; *School of Cybersecurity, University of Chinese Academy of Sciences*; Yueqi Chen and Xinyu Xing, *Pennsylvania State University*; Wei Zou, *Institute of Information Engineering, Chinese Academy of Sciences*; *School of Cybersecurity, University of Chinese Academy of Sciences*

PeX: A Permission Check Analysis Framework for Linux Kernel 1205
Tong Zhang, *Virginia Tech*; Wenbo Shen, *Zhejiang University*; Dongyoon Lee, *Stony Brook University*; Changhee Jung, *Purdue University*; Ahmed M. Azab and Ruowen Wang, *Samsung Research America*

ERIM: Secure, Efficient In-process Isolation with Protection Keys (MPK) 1221
Anjo Vahldiek-Oberwagner, Eslam Elnikety, Nuno O. Duarte, Michael Sammler, Peter Druschel, and Deepak Garg, *Max Planck Institute for Software Systems, Saarland Informatics Campus*

SafeHidden: An Efficient and Secure Information Hiding Technique Using Re-randomization. 1239
Zhe Wang and Chenggang Wu, *State Key Laboratory of Computer Architecture, Institute of Computing Technology, Chinese Academy of Sciences, University of Chinese Academy of Sciences*; Yinqian Zhang, *The Ohio State University*; Bowen Tang, *State Key Laboratory of Computer Architecture, Institute of Computing Technology, Chinese Academy of Sciences, University of Chinese Academy of Sciences*; Pen-Chung Yew, *University of Minnesota at Twin-Cities*; Mengyao Xie, Yuanming Lai, and Yan Kang, *State Key Laboratory of Computer Architecture, Institute of Computing Technology, Chinese Academy of Sciences, University of Chinese Academy of Sciences*; Yueqiang Cheng, *Baidu USA*; Zhiping Shi, *The Capital Normal University*

Exploiting Unprotected I/O Operations in AMD's Secure Encrypted Virtualization. 1257
Mengyuan Li, Yinqian Zhang, and Zhiqiang Lin, *The Ohio State University*; Yan Solihin, *University of Central Florida*

Phishing and Scams

Detecting and Characterizing Lateral Phishing at Scale 1273
Grant Ho, *UC Berkeley and Barracuda Networks*; Asaf Cidon, *Barracuda Networks and Columbia University*; Lior Gavish and Marco Schweighauser, *Barracuda Networks*; Vern Paxson, *UC Berkeley and ICSI*; Stefan Savage and Geoffrey M. Voelker, *UC San Diego*; David Wagner, *UC Berkeley*

High Precision Detection of Business Email Compromise 1291
Asaf Cidon, *Barracuda Networks and Columbia University*; Lior Gavish, Itay Bleier, Nadia Korshun, Marco Schweighauser, and Alexey Tsitkin, *Barracuda Networks*

Cognitive Triaging of Phishing Attacks	1309
Amber van der Heijden and Luca Allodi, <i>Eindhoven University of Technology</i>	
Users Really Do Answer Telephone Scams	1327
Huahong Tu, <i>University of Maryland</i> ; Adam Doupé, <i>Arizona State University</i> ; Ziming Zhao, <i>Rochester Institute of Technology</i> ; Gail-Joon Ahn, <i>Arizona State University and Samsung Research</i>	
Platforms in Everything: Analyzing Ground-Truth Data on the Anatomy and Economics of Bullet-Proof Hosting ..	1341
Arman Noroozian, <i>TU Delft</i> ; Jan Koenders and Eelco van Veldhuizen, <i>Dutch National High-Tech Crime Unit</i> ; Carlos H. Ganan, <i>TU Delft</i> ; Sumayah Alrwais, <i>King Saud University and International Computer Science Institute</i> ; Damon McCoy, <i>New York University</i> ; Michel van Eeten, <i>TU Delft</i>	
Distributed System Security + Verifying Hardware	
Protecting Cloud Virtual Machines from Hypervisor and Host Operating System Exploits.	1357
Shih-Wei Li, John S. Koh, and Jason Nieh, <i>Columbia University</i>	
WAVE: A Decentralized Authorization Framework with Transitive Delegation	1375
Michael P Andersen, Sam Kumar, Moustafa AbdelBaky, Gabe Fierro, John Kolb, Hyung-Sin Kim, David E. Culler, and Raluca Ada Popa, <i>University of California, Berkeley</i>	
in-toto: Providing farm-to-table guarantees for bits and bytes	1393
Santiago Torres-Arias, <i>New York University</i> ; Hammad Afzali, <i>New Jersey Institute of Technology</i> ; Trishank Karthik Kuppusamy, <i>Datadog</i> ; Reza Curtmola, <i>New Jersey Institute of Technology</i> ; Justin Cappos, <i>New York University</i>	
IODINE: Verifying Constant-Time Execution of Hardware	1411
Klaus v. Gleissenthall, Rami Gökhan Kıcı, Deian Stefan, and Ranjit Jhala, <i>University of California, San Diego</i>	
VRASED: A Verified Hardware/Software Co-Design for Remote Attestation	1429
Ivan De Oliveira Nunes, <i>University of California, Irvine</i> ; Karim Eldefrawy, <i>SRI International</i> ; Norrathep Rattanavipanon, <i>University of California, Irvine</i> ; Michael Steiner, <i>Intel</i> ; Gene Tsudik, <i>University of California, Irvine</i>	
Crypto Means Cryptography	
Mobile Private Contact Discovery at Scale.	1447
Daniel Kales and Christian Rechberger, <i>Graz University of Technology</i> ; Thomas Schneider, Matthias Senker, and Christian Weinert, <i>TU Darmstadt</i>	
EverParse: Verified Secure Zero-Copy Parsers for Authenticated Message Formats	1465
Tahina Ramananandro, Antoine Delignat-Lavaud, Cédric Fournet, and Nikhil Swamy, <i>Microsoft Research</i> ; Tej Chajed, <i>MIT</i> ; Nadim Kobeissi, <i>Inria Paris</i> ; Jonathan Protzenko, <i>Microsoft Research</i>	
Blind Bernoulli Trials: A Noninteractive Protocol For Hidden-Weight Coin Flips.	1483
R. Joseph Connor and Max Schuchard, <i>University of Tennessee</i>	
XONN: XNOR-based Oblivious Deep Neural Network Inference	1501
M. Sadegh Riazi and Mohammad Samragh, <i>UC San Diego</i> ; Hao Chen, Kim Laine, and Kristin Lauter, <i>Microsoft Research</i> ; Farinaz Koushanfar, <i>UC San Diego</i>	
JEDI: Many-to-Many End-to-End Encryption and Key Delegation for IoT	1519
Sam Kumar, Yuncong Hu, Michael P Andersen, Raluca Ada Popa, and David E. Culler, <i>University of California, Berkeley</i>	
Passwords	
Birthday, Name and Bifacial-security: Understanding Passwords of Chinese Web Users	1537
Ding Wang and Ping Wang, <i>Peking University</i> ; Debiao He, <i>Wuhan University</i> ; Yuan Tian, <i>University of Virginia</i>	
Protecting accounts from credential stuffing with password breach alerting	1555
Kurt Thomas, Jennifer Pullman, Kevin Yeo, Ananth Raghunathan, Patrick Gage Kelley, Luca Invernizzi, Borbala Benko, Tadek Pietraszek, and Sarvar Patel, <i>Google</i> ; Dan Boneh, <i>Stanford</i> ; Elie Bursztein, <i>Google</i>	

(continued on next page)

Probability Model Transforming Encoders Against Encoding Attacks 1573
Haibo Cheng, Zhixiong Zheng, Wenting Li, and Ping Wang, *Peking University*; Chao-Hsien Chu, *Pennsylvania State University*

Cryptocurrency Scams

The Art of The Scam: Demystifying Honey pots in Ethereum Smart Contracts 1591
Christof Ferreira Torres, Mathis Steichen, and Radu State, *University of Luxembourg*

The Anatomy of a Cryptocurrency Pump-and-Dump Scheme 1609
Jiahua Xu, *École polytechnique fédérale de Lausanne (EPFL)*; Benjamin Livshits, *Imperial College London*

Inadvertently Making Cyber Criminals Rich: A Comprehensive Study of Cryptojacking Campaigns at Internet Scale 1627
Hugo L.J. Bijmans, Tim M. Booi, and Christian Doerr, *Delft University of Technology*

Web Defenses

Rendered Private: Making GLSL Execution Uniform to Prevent WebGL-based Browser Fingerprinting 1645
Shujiang Wu, Song Li, and Yinzhi Cao, *Johns Hopkins University*; Ningfei Wang, *Lehigh University*

Site Isolation: Process Separation for Web Sites within the Browser 1661
Charles Reis, Alexander Moshchuk, and Nasko Oskov, *Google*

Everyone is Different: Client-side Diversification for Defending Against Extension Fingerprinting 1679
Erik Trickel, *Arizona State University*; Oleksii Starov, *Stony Brook University*; Alexandros Kapravelos, *North Carolina State University*; Nick Nikiforakis, *Stony Brook University*; Adam Doupé, *Arizona State University*

Less is More: Quantifying the Security Benefits of Debloating Web Applications 1697
Babak Amin Azad, Pierre Laperdrix, and Nick Nikiforakis, *Stony Brook University*

The Web's Identity Crisis: Understanding the Effectiveness of Website Identity Indicators 1715
Christopher Thompson, Martin Shelton, Emily Stark, Maximilian Walker, Emily Schechter, and Adrienne Porter Felt, *Google*

Software Security

RAZOR: A Framework for Post-deployment Software Debloating 1733
Chenxiong Qian, Hong Hu, Mansour Alharthi, Pak Ho Chung, Taesoo Kim, and Wenke Lee, *Georgia Institute of Technology*

Back to the Whiteboard: a Principled Approach for the Assessment and Design of Memory Forensic Techniques . . 1751
Fabio Pagani and Davide Balzarotti, *EURECOM*

Detecting Missing-Check Bugs via Semantic- and Context-Aware Criticalness and Constraints Inferences 1769
Kangjie Lu, Aditya Pakki, and Qiushi Wu, *University of Minnesota*

DEEPVSA: Facilitating Value-set Analysis with Deep Learning for Postmortem Program Analysis 1787
Wenbo Guo, Dongliang Mu, and Xinyu Xing, *The Pennsylvania State University*; Min Du and Dawn Song, *University of California, Berkeley*

CONFIRM: Evaluating Compatibility and Relevance of Control-flow Integrity Protections for Modern Software . 1805
Xiaoyang Xu, Masoud Ghaffarinia, Wenhao Wang, and Kevin W. Hamlen, *University of Texas at Dallas*; Zhiqiang Lin, *Ohio State University*

Privacy

Point Break: A Study of Bandwidth Denial-of-Service Attacks against Tor 1823
Rob Jansen, *U.S. Naval Research Laboratory*; Tavish Vaidya and Micah Sherr, *Georgetown University*

No Right to Remain Silent: Isolating Malicious Mixes 1841
Hemi Leibowitz, *Bar-Ilan University, IL*; Ania M. Piotrowska and George Danezis, *University College London, UK*; Amir Herzberg, *University of Connecticut, US*

On (The Lack Of) Location Privacy in Crowdsourcing Applications 1859
Spyros Boukoros, *TU-Darmstadt*; Mathias Humbert, *Swiss Data Science Center (ETH Zurich, EPFL)*; Stefan Katzenbeisser, *TU-Darmstadt, University of Passau*; Carmela Troncoso, *EPFL*

Utility-Optimized Local Differential Privacy Mechanisms for Distribution Estimation 1877
Takao Murakami and Yusuke Kawamoto, *AIST*

Evaluating Differentially Private Machine Learning in Practice 1895
Bargav Jayaraman and David Evans, *University of Virginia*

Fuzzing

FUZZIFICATION: Anti-Fuzzing Techniques 1913
Jinho Jung, Hong Hu, David Solodukhin, and Daniel Pagan, *Georgia Institute of Technology*; Kyu Hyung Lee, *University of Georgia*; Taesoo Kim, *Georgia Institute of Technology*

ANTI-FUZZ: Impeding Fuzzing Audits of Binary Executables 1931
Emre Güler, Cornelius Aschermann, Ali Abbasi, and Thorsten Holz, *Ruhr-Universität Bochum*

MOPT: Optimized Mutation Scheduling for Fuzzers 1949
Chenyang Lyu, *Zhejiang University*; Shouling Ji, *Zhejiang University & Alibaba-Zhejiang University Joint Research Institute of Frontier Technologies*; Chao Zhang, *BNRist & INSC, Tsinghua University*; Yuwei Li, *Zhejiang University*; Wei-Han Lee, *IBM Research*; Yu Song, *Zhejiang University*; Raheem Beyah, *Georgia Institute of Technology*

EnFuzz: Ensemble Fuzzing with Seed Synchronization among Diverse Fuzzers 1967
Yuanliang Chen, Yu Jiang, Fuchen Ma, Jie Liang, Mingzhe Wang, and Chijin Zhou, *Tsinghua University*; Xun Jiao, *Villanova University*; Zhuo Su, *Tsinghua University*

GRIMOIRE: Synthesizing Structure while Fuzzing 1985
Tim Blazytko, Cornelius Aschermann, Moritz Schlögel, Ali Abbasi, Sergej Schumilo, Simon Wörner, and Thorsten Holz, *Ruhr-Universität Bochum*