

29th USENIX Security Symposium (USENIX Security'20)

Online
12-14 August 2020

Volume 1 of 4

ISBN: 978-1-7138-1532-7

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© (2020) 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

29th USENIX Security Symposium

August 12–14, 2020

Wednesday, August 12

Wireless Security

- A Formal Analysis of IEEE 802.11's WPA2: Countering the Kracks Caused by Cracking the Counters** 1
Cas Cremers, Benjamin Kiesl, and Niklas Medinger, *CISPA Helmholtz Center for Information Security*
- Frankenstein: Advanced Wireless Fuzzing to Exploit New Bluetooth Escalation Targets** 19
Jan Ruge and Jiska Classen, *Secure Mobile Networking Lab, TU Darmstadt*; Francesco Gringoli, *Dept. of Information Engineering, University of Brescia*; Matthias Hollick, *Secure Mobile Networking Lab, TU Darmstadt*
- Breaking Secure Pairing of Bluetooth Low Energy Using Downgrade Attacks** 37
Yue Zhang, *College of Information Science and Technology, Jinan University (Department of Computer Science, University of Central Florida)*; Jian Weng, *College of Information Science and Technology, Jinan University*; Rajib Dey, *Department of Computer Science, University of Central Florida*; Yier Jin, *Department of Electrical and Computer Engineering, University of Florida*; Zhiqiang Lin, *Computer Science and Engineering, The Ohio State University*; Xinwen Fu, *Department of Computer Science, University of Central Florida*
- You Are What You Broadcast: Identification of Mobile and IoT Devices from (Public) WiFi** 55
Lingjing Yu, *Institute of Information Engineering, Chinese Academy of Sciences*; *School of Cybersecurity, University of the Chinese Academy of Sciences*; Bo Luo, *The University of Kansas*; Jun Ma, *Tsinghua University*; Zhaoyu Zhou and Qingyun Liu, *Institute of Information Engineering, Chinese Academy of Sciences*
- Call Me Maybe: Eavesdropping Encrypted LTE Calls With ReVoLTE** 73
David Rupperecht, Katharina Kohls, and Thorsten Holz, *Ruhr University Bochum*; Christina Pöpper, *NYU Abu Dhabi*

Human Factors

- A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web** 89
Elissa M. Redmiles, Noel Warford, Amritha Jayanti, and Aravind Koneru, *University of Maryland*; Sean Kross, *University of California, San Diego*; Miraida Morales, *Rutgers University*; Rock Stevens and Michelle L. Mazurek, *University of Maryland*
- Understanding security mistakes developers make: Qualitative analysis from Build It, Break It, Fix It** 109
Daniel Votipka, Kelsey R. Fulton, James Parker, Matthew Hou, Michelle L. Mazurek, and Michael Hicks, *University of Maryland*
- Empirical Measurement of Systemic 2FA Usability** 127
Joshua Reynolds, *University of Illinois at Urbana-Champaign and University of California, Berkeley and International Computer Science Institute*; Nikita Samarin, *University of California, Berkeley and International Computer Science Institute*; Joseph Barnes, Taylor Judd, Joshua Mason, and Michael Bailey, *University of Illinois at Urbana-Champaign*; Serge Egelman, *University of California, Berkeley and International Computer Science Institute*
- What Twitter Knows: Characterizing Ad Targeting Practices, User Perceptions, and Ad Explanations Through Users' Own Twitter Data** 145
Miranda Wei, *University of Washington / University of Chicago*; Madison Stamos and Sophie Veys, *University of Chicago*; Nathan Reitinger and Justin Goodman, *University of Maryland*; Margot Herman, *University of Chicago*; Dorota Filipczuk, *University of Southampton*; Ben Weinshel, *University of Chicago*; Michelle L. Mazurek, *University of Maryland*; Blase Ur, *University of Chicago*
- The Impact of Ad-Blockers on Product Search and Purchase Behavior: A Lab Experiment** 163
Alisa Frik, *International Computer Science Institute / UC Berkeley*; Amelia Haviland and Alessandro Acquisti, *Heinz College, Carnegie Mellon University*

Software Security and Verification

- Symbolic execution with SYMCC: Don't interpret, compile!** 181
Sebastian Poeplau and Aurélien Francillon, *EURECOM*

| | |
|--|------------|
| Sys: a Static/Symbolic Tool for Finding Good Bugs in Good (Browser) Code | 199 |
| Fraser Brown, <i>Stanford University</i> ; Deian Stefan, <i>UC San Diego</i> ; Dawson Engler, <i>Stanford University</i> | |
| Everything Old is New Again: Binary Security of WebAssembly | 217 |
| Daniel Lehmann, <i>University of Stuttgart</i> ; Johannes Kinder, <i>Bundeswehr University Munich</i> ; Michael Pradel, <i>University of Stuttgart</i> | |
| AURORA: Statistical Crash Analysis for Automated Root Cause Explanation | 235 |
| Tim Blazytko, Moritz Schlögel, Cornelius Aschermann, Ali Abbasi, Joel Frank, Simon Wörner, and Thorsten Holz, <i>Ruhr-Universität Bochum</i> | |
| SmartVerif: Push the Limit of Automation Capability of Verifying Security Protocols by Dynamic Strategies | 253 |
| Yan Xiong, Cheng Su, Wenchao Huang, Fuyou Miao, Wansen Wang, and Hengyi Ouyang, <i>University of Science and Technology of China</i> | |
| Mobile 1 | |
| BIGMAC: Fine-Grained Policy Analysis of Android Firmware. | 271 |
| Grant Hernandez, <i>University of Florida</i> ; Dave (Jing) Tian, <i>Purdue University</i> ; Anurag Swarnim Yadav, Byron J. Williams, and Kevin R.B. Butler, <i>University of Florida</i> | |
| From Needs to Actions to Secure Apps? The Effect of Requirements and Developer Practices on App Security . . . | 289 |
| Charles Weir, <i>Lancaster University</i> ; Ben Hermann, <i>Paderborn University</i> ; Sascha Fahl, <i>Leibniz University Hannover</i> | |
| FANS: Fuzzing Android Native System Services via Automated Interface Analysis | 307 |
| Baozheng Liu and Chao Zhang, <i>Institute of Network Science and Cyberspace, Tsinghua University; Beijing National Research Center for Information Science and Technology</i> ; Guang Gong, <i>Alpha Lab, 360 Internet Security Center</i> ; Yishun Zeng, <i>Institute of Network Science and Cyberspace, Tsinghua University; Beijing National Research Center for Information Science and Technology</i> ; Haifeng Ruan, <i>Department of Computer Science and Technology, Tsinghua University</i> ; Jianwei Zhuge, <i>Institute of Network Science and Cyberspace, Tsinghua University; Beijing National Research Center for Information Science and Technology</i> | |
| Chaperone: Real-time Locking and Loss Prevention for Smartphones | 325 |
| Jiayi Chen and Urs Hengartner, <i>Cheriton School of Computer Science, University of Waterloo</i> ; Hassan Khan, <i>School of Computer Science, University of Guelph</i> ; Mohammad Mannan, <i>Concordia Institute for Information Systems Engineering, Concordia University</i> | |
| Towards HTTPS Everywhere on Android: We Are Not There Yet. | 343 |
| Andrea Possemato, <i>EURECOM / IDEMIA</i> ; Yanick Fratantonio, <i>EURECOM</i> | |
| Phishing, Spam, and Threat Intelligence | |
| Sunrise to Sunset: Analyzing the End-to-end Life Cycle and Effectiveness of Phishing Attacks at Scale | 361 |
| Adam Oest and Penghui Zhang, <i>Arizona State University</i> ; Brad Wardman, Eric Nunes, and Jakub Burgis, <i>PayPal</i> ; Ali Zand and Kurt Thomas, <i>Google</i> ; Adam Doupé, <i>Arizona State University</i> ; Gail-Joon Ahn, <i>Arizona State University, Samsung Research</i> | |
| PhishTime: Continuous Longitudinal Measurement of the Effectiveness of Anti-phishing Blacklists | 379 |
| Adam Oest, Yeganeh Safaei, and Penghui Zhang, <i>Arizona State University</i> ; Brad Wardman and Kevin Tyers, <i>PayPal</i> ; Yan Shoshitaishvili and Adam Doupé, <i>Arizona State University</i> ; Gail-Joon Ahn, <i>Arizona State University, Samsung Research</i> | |
| Who's Calling? Characterizing Robocalls through Audio and Metadata Analysis. | 397 |
| Sathvik Prasad, Elijah Bouma-Sims, Athishay Kiran Mylappan, and Bradley Reaves, <i>North Carolina State University</i> | |
| See No Evil: Phishing for Permissions with False Transparency | 415 |
| Güliz Seray Tuncay, <i>Google, University of Illinois at Urbana-Champaign</i> ; Jingyu Qian and Carl A. Gunter, <i>University of Illinois at Urbana-Champaign</i> | |
| A different cup of TI? The added value of commercial threat intelligence. | 433 |
| Xander Bouwman, <i>Delft University of Technology, the Netherlands</i> ; Harm Griffioen, <i>Hasso Plattner Institute, University of Potsdam, Germany</i> ; Jelle Egbers, <i>Delft University of Technology, the Netherlands</i> ; Christian Doerr, <i>Hasso Plattner Institute, University of Potsdam, Germany</i> ; Bram Klievink, <i>Leiden University, the Netherlands</i> ; Michel van Eeten, <i>Delft University of Technology, the Netherlands</i> | |

Trusted Execution Environments 1

- HYBCACHE: Hybrid Side-Channel-Resilient Caches for Trusted Execution Environments** 451
Ghada Dessouky, Tommaso Frassetto, and Ahmad-Reza Sadeghi, *Technische Universität Darmstadt*
- COPYCAT: Controlled Instruction-Level Attacks on Enclaves** 469
Daniel Moghimi, *Worcester Polytechnic Institute*; Jo Van Bulck, *KU Leuven*; Nadia Heninger, *University of California, San Diego, CA, USA*; Frank Piessens, *KU Leuven*; Berk Sunar, *Worcester Polytechnic Institute*
- An Off-Chip Attack on Hardware Enclaves via the Memory Bus** 487
Dayeol Lee, *UC Berkeley*; Dongha Jung, *SK Hynix*; Ian T. Fang, *UC Berkeley*; Chia-Che Tsai, *Texas A&M University*; Raluca Ada Popa, *UC Berkeley*
- Civet: An Efficient Java Partitioning Framework for Hardware Enclaves** 505
Chia-Che Tsai, *Texas A&M University*; Jeongseok Son, *UC Berkeley*; Bhushan Jain, *The University of North Carolina at Chapel Hill*; John McAvey, *Hendrix College*; Raluca Ada Popa, *UC Berkeley*; Donald E. Porter, *The University of North Carolina at Chapel Hill*
- BesFS: A POSIX Filesystem for Enclaves with a Mechanized Safety Proof** 523
Shweta Shinde, *University of California, Berkeley*; Shengyi Wang and Pinghai Yuan, *National University of Singapore*; Aquinas Hobor, *National University of Singapore & Yale-NUS College*; Abhik Roychoudhury and Prateek Saxena, *National University of Singapore*

Network Security

- EPIC: Every Packet Is Checked in the Data Plane of a Path-Aware Internet** 541
Markus Legner, Tobias Klenze, Marc Wyss, Christoph Sprenger, and Adrian Perrig, *ETH Zurich*
- ShadowMove: A Stealthy Lateral Movement Strategy** 559
Amirreza Niakanlahiji, *University of Illinois Springfield*; Jinpeng Wei and Md Rabbi Alam, *UNC Charlotte*; Qingyang Wang, *Louisiana State University*; Bei-Tseng Chu, *UNC Charlotte*
- Poison Over Troubled Forwarders: A Cache Poisoning Attack Targeting DNS Forwarding Devices** 577
Xiaofeng Zheng, *Tsinghua University*; Qi An Xin Technology Research Institute; Chaoyi Lu and Jian Peng, *Tsinghua University*; Qiushi Yang, *Qi An Xin Technology Research Institute*; Dongjie Zhou, *State Key Laboratory of Mathematical Engineering and Advanced Computing*; Baojun Liu, *Tsinghua University*; Keyu Man, *University of California, Riverside*; Shuang Hao, *University of Texas at Dallas*; Haixin Duan, *Tsinghua University*; Qi An Xin Technology Research Institute; Zhiyun Qian, *University of California, Riverside*
- Programmable In-Network Security for Context-aware BYOD Policies** 595
Qiao Kang, *Rice University*; Lei Xue, *The Hong Kong Polytechnic University*; Adam Morrison, Yuxin Tang, and Ang Chen, *Rice University*; Xiapu Luo, *The Hong Kong Polytechnic University*
- A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email** 613
Hyeonmin Lee, *Seoul National University*; Aniketh Gireesh, *Amrita Vishwa Vidyapeetham*; Roland van Rijswijk-Deij, *University of Twente & NLnet Labs*; Taekyoung “Ted” Kwon, *Seoul National University*; Taejoong Chung, *Rochester Institute of Technology*
- NXNSAttack: Recursive DNS Inefficiencies and Vulnerabilities** 631
Yehuda Afek, *Tel-Aviv University*; Anat Bremler-Barr, *IDC*; Lior Shafir, *Tel Aviv University*

Web Security and Privacy

- Shim Shimmeny: Evaluating the Security and Privacy Contributions of Link Shimming in the Modern Web** 649
Frank Li, *Georgia Institute of Technology / Facebook*
- Cached and Confused: Web Cache Deception in the Wild** 665
Seyed Ali Mirheidari, *University of Trento*; Sajjad Arshad, *Northeastern University*; Kaan Onarlioglu, *Akamai Technologies*; Bruno Crispo, *University of Trento, KU Leuven*; Engin Kirda and William Robertson, *Northeastern University*
- A Tale of Two Headers: A Formal Analysis of Inconsistent Click-Jacking Protection on the Web** 683
Stefano Calzavara, *Università Ca’ Foscari Venezia*; Sebastian Roth, *CISPA Helmholtz Center for Information Security and Saarbrücken Graduate School of Computer Science*; Alvise Rabitti, *Università Ca’ Foscari Venezia*; Michael Backes and Ben Stock, *CISPA Helmholtz Center for Information Security*

| | |
|--|------------|
| Retrofitting Fine Grain Isolation in the Firefox Renderer | 699 |
| Shravan Narayan and Craig Disselkoen, <i>UC San Diego</i> ; Tal Garfinkel, <i>Stanford University</i> ; Nathan Froyd and Eric Rahm, <i>Mozilla</i> ; Sorin Lerner, <i>UC San Diego</i> ; Hovav Shacham, <i>UT Austin</i> ; Deian Stefan, <i>UC San Diego</i> | |
| Zero-delay Lightweight Defenses against Website Fingerprinting | 717 |
| Jiajun Gong and Tao Wang, <i>Hong Kong University of Science and Technology</i> | |
| Achieving Keyless CDNs with Conclaves | 735 |
| Stephen Herwig, <i>University of Maryland</i> ; Christina Garman, <i>Purdue University</i> ; Dave Levin, <i>University of Maryland</i> | |
| Trusted Execution Environments 2 | |
| SENG, the SGX-Enforcing Network Gateway: Authorizing Communication from Shielded Clients | 753 |
| Fabian Schwarz and Christian Rossow, <i>CISPA Helmholtz Center for Information Security</i> | |
| APEX: A Verified Architecture for Proofs of Execution on Remote Devices under Full Software Compromise | 771 |
| Ivan De Oliveira Nunes, <i>UC Irvine</i> ; Karim Eldefrawy, <i>SRI International</i> ; Norrathep Rattanavipanon, <i>UC Irvine and Prince of Songkla University</i> ; Gene Tsudik, <i>UC Irvine</i> | |
| PARTEMU: Enabling Dynamic Analysis of Real-World TrustZone Software Using Emulation | 789 |
| Lee Harrison and Hayawardh Vijayakumar, <i>Samsung Knox, Samsung Research America</i> ; Rohan Padhye and Koushik Sen, <i>EECS Department, University of California, Berkeley</i> ; Michael Grace, <i>Samsung Knox, Samsung Research America</i> | |
| PHMon: A Programmable Hardware Monitor and Its Security Use Cases. | 807 |
| Leila Delshadtehrani, Sadullah Canakci, Boyou Zhou, Schuyler Eldridge, Ajay Joshi, and Manuel Egele, <i>Boston University</i> | |
| Horizontal Privilege Escalation in Trusted Applications. | 825 |
| Darius Suci, <i>Stony Brook University</i> ; Stephen McLaughlin and Laurent Simon, <i>Samsung Research America</i> ; Radu Sion, <i>Stony Brook University</i> | |
| TEEREX: Discovery and Exploitation of Memory Corruption Vulnerabilities in SGX Enclaves. | 841 |
| Tobias Cloosters, Michael Rodler, and Lucas Davi, <i>University of Duisburg-Essen</i> | |

Thursday, August 13

Automotive and Drone Security

| | |
|---|------------|
| Stealthy Tracking of Autonomous Vehicles with Cache Side Channels | 859 |
| Mulong Luo, Andrew C. Myers, and G. Edward Suh, <i>Cornell University</i> | |
| Towards Robust LiDAR-based Perception in Autonomous Driving: General Black-box Adversarial Sensor Attack and Countermeasures. | 877 |
| Jiachen Sun and Yulong Cao, <i>University of Michigan</i> ; Qi Alfred Chen, <i>UC Irvine</i> ; Z. Morley Mao, <i>University of Michigan</i> | |
| SAVIOR: Securing Autonomous Vehicles with Robust Physical Invariants. | 895 |
| Raul Quinonez, <i>University of Texas at Dallas</i> ; Jairo Giraldo, <i>University of Utah</i> ; Luis Salazar, <i>University of California, Santa Cruz</i> ; Erick Bauman, <i>University of Texas at Dallas</i> ; Alvaro Cardenas, <i>University of California, Santa Cruz</i> ; Zhiqiang Lin, <i>Ohio State University</i> | |
| From Control Model to Program: Investigating Robotic Aerial Vehicle Accidents with MAYDAY. | 913 |
| Taegy Kim, <i>Purdue University</i> ; Chung Hwan Kim, <i>University of Texas at Dallas</i> ; Altay Ozen, Fan Fei, Zhan Tu, Xiangyu Zhang, Xinyan Deng, Dave (Jing) Tian, and Dongyan Xu, <i>Purdue University</i> | |
| Drift with Devil: Security of Multi-Sensor Fusion based Localization in High-Level Autonomous Driving under GPS Spoofing | 931 |
| Junjie Shen, Jun Yeon Won, Zeyuan Chen, and Qi Alfred Chen, <i>University of California, Irvine</i> | |
| Plug-N-Pwned: Comprehensive Vulnerability Analysis of OBD-II Dongles as A New Over-the-Air Attack Surface in Automotive IoT | 949 |
| Haohuang Wen, <i>Ohio State University</i> ; Qi Alfred Chen, <i>University of California, Irvine</i> ; Zhiqiang Lin, <i>Ohio State University</i> | |

Privacy Enhancing Technologies

CKV: Locally Differentially Private Correlated Key-Value Data Collection with Optimized Utility 967
Xiaolan Gu and Ming Li, *University of Arizona*; Yueqiang Cheng, *Baidu X-Lab*; Li Xiong, *Emory University*; Yang Cao, *Kyoto University*

Actions Speak Louder than Words: Entity-Sensitive Privacy Policy and Data Flow Analysis with POLICHECK. 985
Benjamin Andow, *IBM T.J. Watson Research Center*; Samin Yaseer Mahmud, Justin Whitaker, William Enck, and Bradley Reaves, *North Carolina State University*; Kapil Singh, *IBM T.J. Watson Research Center*; Serge Egelman, *U.C. Berkeley / ICSI / AppCensus Inc.*

Walking Onions: Scaling Anonymity Networks while Protecting Users. 1003
Chelsea H. Komlo, *University of Waterloo*; Nick Mathewson, *The Tor Project*; Ian Goldberg, *University of Waterloo*

Differentially-Private Control-Flow Node Coverage for Software Usage Analysis1021
Hailong Zhang, Sufian Latif, Raef Bassily, and Atanas Rountev, *The Ohio State University*

Visor: Privacy-Preserving Video Analytics as a Cloud Service. 1039
Rishabh Poddar, *UC Berkeley and Microsoft Research*; Ganesh Ananthanarayanan, Srinath Setty, and Stavros Volos, *Microsoft Research*; Raluca Ada Popa, *UC Berkeley*

DELf: Safeguarding deletion correctness in Online Social Networks 1057
Katriel Cohn-Gordon, *Facebook*; Georgios Damaskinos, *Facebook, EPFL*; Divino Neto, Joshi Cordova, Benoît Reitz, Benjamin Strahs, and Daniel Obenshain, *Facebook*; Paul Pearce, *Facebook, Georgia Tech*; Ioannis Papagiannis, *Facebook*

Software Security

Datalog Disassembly 1075
Antonio Flores-Montoya and Eric Schulte, *GrammarTech Inc.*

KOOBE: Towards Facilitating Exploit Generation of Kernel Out-Of-Bounds Write Vulnerabilities. 1093
Weiteng Chen, Xiaochen Zou, Guoren Li, and Zhiyun Qian, *UC Riverside*

Automatic Techniques to Systematically Discover New Heap Exploitation Primitives1111
Insu Yun, *Georgia Institute of Technology*; Dhaval Kapil, *Facebook*; Taesoo Kim, *Georgia Institute of Technology*

The Industrial Age of Hacking 1129
Timothy Nosco, *United States Army*; Jared Ziegler, *National Security Agency*; Zechariah Clark and Davy Marrero, *United States Navy*; Todd Finkler, *United States Air Force*; Andrew Barbarello, *United States Navy*; W. Michael Petullo, *United States Army*

BScout: Direct Whole Patch Presence Test for Java Executables1147
Jiarun Dai, Yuan Zhang, Zheyue Jiang, Yingtian Zhou, and Junyan Chen, *Fudan University*; Xinyu Xing, *Pennsylvania State University*; Xiaohan Zhang, Xin Tan, Min Yang, and Zhemin Yang, *Fudan University*

MVP: Detecting Vulnerabilities using Patch-Enhanced Vulnerability Signatures1165
Yang Xiao, *Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China and School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China*; Bihuan Chen, *School of Computer Science and Shanghai Key Laboratory of Data Science, Fudan University, China*; Chendong Yu, *Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China and School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China*; Zhengzi Xu, *School of Computer Science and Engineering, Nanyang Technological University, Singapore*; Zimu Yuan, Feng Li, and Binghong Liu, *Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China and School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China*; Yang Liu, *School of Computer Science and Engineering, Nanyang Technological University, Singapore*; Wei Huo and Wei Zou, *Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China and School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China*; Wenchang Shi, *Renmin University of China, Beijing, China*

Embedded/IoT Security

Shattered Chain of Trust: Understanding Security Risks in Cross-Cloud IoT Access Delegation 1183

Bin Yuan, *School of Cyber Science and Engineering, Huazhong Univ. of Sci. & Tech., China; National Engineering Research Center for Big Data Technology and System, Cluster and Grid Computing Lab, Services Computing Technology and System Lab, and Big Data Security Engineering Research Center, Huazhong Univ. of Sci. & Tech., China; Shenzhen Huazhong University of Science and Technology Research Institute, China; Indiana University Bloomington*; Yan Jia, *School of Cyber Engineering, Xidian University, China; National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, China; Indiana University Bloomington*; Luyi Xing, Dongfang Zhao, and XiaoFeng Wang, *Indiana University Bloomington*; Deqing Zou, *School of Cyber Science and Engineering, Huazhong Univ. of Sci. & Tech., China; National Engineering Research Center for Big Data Technology and System, Cluster and Grid Computing Lab, Services Computing Technology and System Lab, and Big Data Security Engineering Research Center, Huazhong Univ. of Sci. & Tech., China*; Hai Jin, *School of Computer Science and Technology, Huazhong Univ. of Sci. & Tech., China; National Engineering Research Center for Big Data Technology and System, Cluster and Grid Computing Lab, Services Computing Technology and System Lab, and Big Data Security Engineering Research Center, Huazhong Univ. of Sci. & Tech., China*; Yuqing Zhang, *National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, China; School of Cyber Engineering, Xidian University, China*

HALucinator: Firmware Re-hosting Through Abstraction Layer Emulation. 1201

Abraham A Clements, *Sandia National Laboratories*; Eric Gustafson, *UC Santa Barbara and Sandia National Laboratories*; Tobias Scharnowski, *Ruhr-Universität Bochum*; Paul Groesen, *UC Santa Barbara*; David Fritz, *Sandia National Laboratories*; Christopher Kruegel and Giovanni Vigna, *UC Santa Barbara*; Saurabh Bagchi, *Purdue University*; Mathias Payer, *EPFL*

Silhouette: Efficient Protected Shadow Stacks for Embedded Systems 1219

Jie Zhou, Yufei Du, and Zhuojia Shen, *University of Rochester*; Lele Ma, *University of Rochester and College of William and Mary*; John Criswell, *University of Rochester*; Robert J. Walls, *Worcester Polytechnic Institute*

P²IM: Scalable and Hardware-independent Firmware Testing via Automatic Peripheral Interface Modeling . . . 1237

Bo Feng, Alejandro Mera, and Long Lu, *Northeastern University*

COUNTERFOIL: Verifying Provenance of Integrated Circuits using Intrinsic Package Fingerprints and Inexpensive Cameras 1255

Siva Nishok Dhanuskodi, Xiang Li, and Daniel Holcomb, *University of Massachusetts Amherst*

Hall Spoofing: A Non-Invasive DoS Attack on Grid-Tied Solar Inverter. 1273

Anomadarshi Barua and Mohammad Abdullah Al Faruque, *UC Irvine*

Machine Learning 1

Updates-Leak: Data Set Inference and Reconstruction Attacks in Online Learning 1291

Ahmed Salem, *CISPA Helmholtz Center for Information Security*; Apratim Bhattacharya, *Max Planck Institute for Informatics*; Michael Backes, Mario Fritz, and Yang Zhang, *CISPA Helmholtz Center for Information Security*

Exploring Connections Between Active Learning and Model Extraction 1309

Varun Chandrasekaran, *University of Wisconsin-Madison*; Kamalika Chaudhuri, *University of California San Diego*; Irene Giacomelli, *Protocol Labs*; Somesh Jha, *University of Wisconsin-Madison*; Songbai Yan, *University of California San Diego*

Hybrid Batch Attacks: Finding Black-box Adversarial Examples with Limited Queries. 1327

Fnu Suya, Jianfeng Chi, David Evans, and Yuan Tian, *University of Virginia*

High Accuracy and High Fidelity Extraction of Neural Networks 1345

Matthew Jagielski, *Northeastern University, Google Brain*; Nicholas Carlini, David Berthelot, Alex Kurakin, and Nicolas Papernot, *Google Brain*

Adversarial Preprocessing: Understanding and Preventing Image-Scaling Attacks in Machine Learning. 1363

Erwin Quiring, David Klein, Daniel Arp, Martin Johns, and Konrad Rieck, *TU Braunschweig*

TEXTSHIELD: Robust Text Classification Based on Multimodal Embedding and Neural Machine Translation . . . 1381

Jinfeng Li, *Zhejiang University, Alibaba Group*; Tianyu Du, *Zhejiang University*; Shouling Ji, *Zhejiang University, Alibaba-Zhejiang University Joint Research Institute of Frontier Technologies*; Rong Zhang and Quan Lu, *Alibaba Group*; Min Yang, *Fudan University*; Ting Wang, *Pennsylvania State University*

Microarchitectural Attacks

- Data Recovery from “Scrubbed” NAND Flash Storage: Need for Analog Sanitization** 1399
Md Mehedi Hasan and Biswajit Ray, *The University of Alabama in Huntsville*
- PKU Pitfalls: Attacks on PKU-based Memory Isolation Systems** 1409
R. Joseph Connor, Tyler McDaniel, Jared M. Smith, and Max Schuchard, *University of Tennessee, Knoxville*
- Medusa: Microarchitectural Data Leakage via Automated Attack Synthesis**1427
Daniel Moghimi, *Worcester Polytechnic Institute*; Moritz Lipp, *Graz University of Technology*; Berk Sunar, *Worcester Polytechnic Institute*; Michael Schwarz, *Graz University of Technology*
- VOLTPwn: Attacking x86 Processor Integrity from Software** 1445
Zijo Kenjar and Tommaso Frassetto, *Technische Universität Darmstadt*; David Gens and Michael Franz, *University of California, Irvine*; Ahmad-Reza Sadeghi, *Technische Universität Darmstadt*
- DeepHammer: Depleting the Intelligence of Deep Neural Networks through Targeted Chain of Bit Flips** 1463
Fan Yao, *University of Central Florida*; Adnan Siraj Rakin and Deliang Fan, *Arizona State University*
- SpecFuzz: Bringing Spectre-type vulnerabilities to the surface** 1481
Oleksii Oleksenko and Bohdan Trach, *TU Dresden*; Mark Silberstein, *Technion*; Christof Fetzer, *TU Dresden*

Financial Tech and Voting

- Security Analysis of Unified Payments Interface and Payment Apps in India** 1499
Renuka Kumar, *University of Michigan*; Sreesh Kishore; Hao Lu and Atul Prakash, *University of Michigan*
- Cardpliance: PCI DSS Compliance of Android Applications**1517
Samin Yaseer Mahmud and Akhil Acharya, *North Carolina State University*; Benjamin Andow, *IBM T.J. Watson Research Center*; William Enck and Bradley Reaves, *North Carolina State University*
- The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections** 1535
Michael A. Specter, James Koppel, and Daniel Weitzner, *MIT*
- VOTEAGAIN: A scalable coercion-resistant voting system** 1553
Wouter Lueks, *EPFL*; Iñigo Querejeta-Azurmendi, *Universidad Carlos III Madrid/ITEFI, CSIC*; Carmela Troncoso, *EPFL*
- Boxer: Preventing fraud by scanning credit cards** 1571
Zainul Abi Din and Hari Venugopalan, *UC Davis*; Jaime Park, *Bouncer Technologies*; Andy Li, *Segment*; Weisu Yin, *UC Davis*; Haohui Mai, *Hengmuxing Technologies*; Yong Jae Lee, *UC Davis*; Steven Liu, *Bouncer Technologies*; Samuel T. King, *UC Davis and Bouncer Technologies*

Machine Learning 2

- Fawkes: Protecting Privacy against Unauthorized Deep Learning Models** 1589
Shawn Shan, Emily Wenger, Jiayun Zhang, Huiying Li, Haitao Zheng, and Ben Y. Zhao, *University of Chicago*
- Stolen Memories: Leveraging Model Memorization for Calibrated White-Box Membership Inference** 1605
Klas Leino and Matt Fredrikson, *Carnegie Mellon University*
- Local Model Poisoning Attacks to Byzantine-Robust Federated Learning** 1623
Minghong Fang, *Iowa State University*; Xiaoyu Cao, Jinyuan Jia, and Neil Gong, *Duke University*
- Justinian’s GAAvernor: Robust Distributed Learning with Gradient Aggregation Agent**1641
Xudong Pan, Mi Zhang, Duocai Wu, and Qifan Xiao, *Fudan University*; Shouling Ji, *Zhejiang University/Ant Financial*; Min Yang, *Fudan University*
- Interpretable Deep Learning under Fire** 1659
Xinyang Zhang, *Pennsylvania State University*; Ningfei Wang, *University of California Irvine*; Hua Shen, *Pennsylvania State University*; Shouling Ji, *Zhejiang University and Alibaba-ZJU Joint Institute of Frontier Technologies*; Xiapu Luo, *Hong Kong Polytechnic University*; Ting Wang, *Pennsylvania State University*

Systems Security

- Donky: Domain Keys – Efficient In-Process Isolation for RISC-V and x86.** 1677
David Schrammel, Samuel Weiser, Stefan Steinegger, Martin Schwarzl, Michael Schwarz, Stefan Mangard, and Daniel Gruss, *Graz University of Technology*
- (Mostly) Exitless VM Protection from Untrusted Hypervisor through Disaggregated Nested Virtualization.**1695
Zeyu Mi, Dingji Li, Haibo Chen, Binyu Zang, and Haibing Guan, *Shanghai Key Laboratory for Scalable Computing Systems, School of Software, Shanghai Jiao Tong University*
- DECAF: Automatic, Adaptive De-bloating and Hardening of COTS Firmware.**1713
Jake Christensen, *Private Machines*; Ionut Mugurel Anghel, *Univ. Politehnica Bucharest*; Rob Taglang, *Private Machines*; Mihai Chiroiu, *Univ. Politehnica Bucharest*; Radu Sion, *Private Machines*
- McTiny: Fast High-Confidence Post-Quantum Key Erasure for Tiny Network Servers**1731
Daniel J. Bernstein, *University of Illinois at Chicago, Ruhr University Bochum*; Tanja Lange, *Eindhoven University of Technology*
- Temporal System Call Specialization for Attack Surface Reduction**1749
Seyedhamed Ghavamnia, Tapti Palit, Shachee Mishra, and Michalis Polychronakis, *Stony Brook University*

Friday, August 14

Analysis of Crypto

- Big Numbers - Big Troubles: Systematically Analyzing Nonce Leakage in (EC)DSA Implementations**1767
Samuel Weiser, David Schrammel, and Lukas Bodner, *Graz University of Technology*; Raphael Spreitzer, *SGS Digital Trust Services*
- Estonian Electronic Identity Card: Security Flaws in Key Management**1785
Arnis Parsovs, *Software Technology and Applications Competence Center and University of Tartu*
- The Unpatchable Silicon: A Full Break of the Bitstream Encryption of Xilinx 7-Series FPGAs.** 1803
Maik Ender and Amir Moradi, *Horst Goertz Institute for IT Security, Ruhr University Bochum, Germany*; Christof Paar, *Max Planck Institute for Cyber Security and Privacy and Horst Goertz Institute for IT Security, Ruhr University Bochum, Germany*
- Automating the Development of Chosen Ciphertext Attacks.**1821
Gabrielle Beck, Maximilian Zinkus, and Matthew Green, *Johns Hopkins University*
- SHA-1 is a Shambles: First Chosen-Prefix Collision on SHA-1 and Application to the PGP Web of Trust.** 1839
Gaëtan Leurent, *Inria, France*; Thomas Peyrin, *Nanyang Technological University, Singapore*
- A Spectral Analysis of Noise: A Comprehensive, Automated, Formal Analysis of Diffie-Hellman Protocols** 1857
Guillaume Girol, *CEA, List, Université Paris-Saclay, France*; Lucca Hirschi, *Inria & LORIA, France*; Ralf Sasse, *Department of Computer Science, ETH Zurich*; Dennis Jackson, *University of Oxford, United Kingdom*; Cas Cremers, *CISPA Helmholtz Center for Information Security*; David Basin, *Department of Computer Science, ETH Zurich*

Specific User Populations

- An Observational Investigation of Reverse Engineers' Processes**1875
Daniel Votipka and Seth Rabin, *University of Maryland*; Kristopher Micinski, *Syracuse University*; Jeffrey S. Foster, *Tufts University*; Michelle L. Mazurek, *University of Maryland*
- The Tools and Tactics Used in Intimate Partner Surveillance: An Analysis of Online Infidelity Forums** 1893
Emily Tseng, *Cornell University*; Rosanna Bellini, *Open Lab, Newcastle University*; Nora McDonald, *University of Maryland, Baltimore County*; Matan Danos, *Weizmann Institute of Science*; Rachel Greenstadt and Damon McCoy, *New York University*; Nicola Dell and Thomas Ristenpart, *Cornell Tech*
- DATASHARENETWORK: A Decentralized Privacy-Preserving Search Engine for Investigative Journalists** 1911
Kasra Edalatnejad and Wouter Lueks, *EPFL*; Julien Pierre Martin; Soline Ledésert, Anne L'Hôte, and Bruno Thomas, *ICIJ*; Laurent Girod and Carmela Troncoso, *EPFL*

“I am uncomfortable sharing what I can’t see”: Privacy Concerns of the Visually Impaired with Camera Based Assistive Applications 1929
Taslima Akter, *Indiana University Bloomington*; Bryan Dosono, *Syracuse University*; Tousif Ahmed and Apu Kapadia, *Indiana University Bloomington*; Bryan Semaan, *Syracuse University*

‘I have too much respect for my elders’: Understanding South African Mobile Users’ Perceptions of Privacy and Current Behaviors on Facebook and WhatsApp 1949
Jake Reichel, Fleming Peck, Mikako Inaba, Bisrat Moges, and Brahmnoor Singh Chawla, *Princeton University*; Marshini Chetty, *University of Chicago*

Side Channel Attacks

RELOAD+REFRESH: Abusing Cache Replacement Policies to Perform Stealthy Cache Attacks 1967
Samira Briongos, Pedro Malagón, and José M. Moya, *Integrated Systems Laboratory, Universidad Politécnica de Madrid*; Thomas Eisenbarth, *University of Lübeck and Worcester Polytechnic Institute*

Timeless Timing Attacks: Exploiting Concurrency to Leak Secrets over Remote Connections 1985
Tom Van Goethem, *imec-DistriNet, KU Leuven*; Christina Pöpper, *New York University Abu Dhabi*; Wouter Joosen, *imec-DistriNet, KU Leuven*; Mathy Vanhoef, *New York University Abu Dhabi*

Cache Telepathy: Leveraging Shared Resource Attacks to Learn DNN Architectures 2003
Mengjia Yan, Christopher W. Fletcher, and Josep Torrellas, *University of Illinois at Urbana-Champaign*

Certified Side Channels 2021
Cesar Pereida García, Sohaib ul Hassan, Nicola Tuveri, and Iaroslav Gridin, *Tampere University*; Alejandro Cabrera Aldaya, *Tampere University and Universidad Tecnológica de la Habana*; Billy Bob Brumley, *Tampere University*

NetWarden: Mitigating Network Covert Channels while Preserving Performance 2039
Jiarong Xing, Qiao Kang, and Ang Chen, *Rice University*

TPM-FAIL: TPM meets Timing and Lattice Attacks 2057
Daniel Moghimi and Berk Sunar, *Worcester Polytechnic Institute, Worcester, MA, USA*; Thomas Eisenbarth, *University of Lübeck, Lübeck, Germany*; Nadia Heninger, *University of California, San Diego, CA, USA*

Implementations of Crypto

Scaling Verifiable Computation Using Efficient Set Accumulators 2075
Alex Ozdemir and Riad Wahby, *Stanford University*; Barry Whitehat, *Unaffiliated*; Dan Boneh, *Stanford University*

Pixel: Multi-signatures for Consensus 2093
Manu Drijvers, *DFINITY*; Sergey Gorbunov, *Algorand and University of Waterloo*; Gregory Neven, *DFINITY*; Hoeteck Wee, *Algorand and CNRS, ENS, PSL*

SANNS: Scaling Up Secure Approximate k -Nearest Neighbors Search2111
Hao Chen, *Microsoft Research*; Iliaria Chillotti, *imec-COSIC KU Leuven & Zama*; Yihe Dong, *Microsoft*; Oxana Poburinnaya, *Simons Institute*; Ilya Razenshteyn, *Microsoft Research*; M. Sadegh Riazi, *UC San Diego*

MIRAGE: Succinct Arguments for Randomized Algorithms with Applications to Universal zk-SNARKs 2129
Ahmed Kosba, *Alexandria University*; Dimitrios Papadopoulos, *Hong Kong University of Science and Technology*; Charalampos Papamanthou, *University of Maryland*; Dawn Song, *UC Berkeley*

Secure Multi-party Computation of Differentially Private Median2147
Jonas Böhler, *SAP Security Research*; Florian Kerschbaum, *University of Waterloo*

Authentication

That Was Then, This Is Now: A Security Evaluation of Password Generation, Storage, and Autofill in Browser-Based Password Managers2165
Sean Oesch and Scott Ruoti, *University of Tennessee*

Composition Kills: A Case Study of Email Sender Authentication 2183
Jianjun Chen, *International Computer Science Institute*; Vern Paxson, *University of California Berkeley and International Computer Science Institute*; Jian Jiang, *Shape Security*

| | |
|---|-------------|
| Detecting Stuffing of a User’s Credentials at Her Own Accounts | 2201 |
| Ke Coby Wang and Michael K. Reiter, <i>University of North Carolina at Chapel Hill</i> | |
| Liveness is Not Enough: Enhancing Fingerprint Authentication with Behavioral Biometrics to Defeat Puppet Attacks | 2219 |
| Cong Wu, Kun He, and Jing Chen, <i>Wuhan University</i> ; Ziming Zhao, <i>Rochester Institute of Technology</i> ; Ruiying Du, <i>Wuhan University</i> | |
| Human Distinguishable Visual Key Fingerprints | 2237 |
| Mozhgan Azimpourkivi and Umut Topkara, <i>Bloomberg</i> ; Bogdan Carbutar, <i>FIU</i> | |
| Fuzzing 1 | |
| FuzzGuard: Filtering out Unreachable Inputs in Directed Grey-box Fuzzing through Deep Learning. | 2255 |
| Peiyuan Zong, Tao Lv, Dawei Wang, Zizhuang Deng, Ruigang Liang, and Kai Chen, <i>SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China</i> | |
| FuzzGen: Automatic Fuzzer Generation | 2271 |
| Kyriakos Ispoglou, Daniel Austin, and Vishwath Mohan, <i>Google Inc.</i> ; Mathias Payer, <i>EPFL</i> | |
| ParmeSan: Sanitizer-guided Greybox Fuzzing | 2289 |
| Sebastian Österlund, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida, <i>Vrije Universiteit Amsterdam</i> | |
| EcoFuzz: Adaptive Energy-Saving Greybox Fuzzing as a Variant of the Adversarial Multi-Armed Bandit | 2307 |
| Tai Yue, Pengfei Wang, Yong Tang, Enze Wang, Bo Yu, Kai Lu, and Xu Zhou, <i>National University of Defense Technology</i> | |
| Muzz: Thread-aware Grey-box Fuzzing for Effective Bug Hunting in Multithreaded Programs | 2325 |
| Hongxu Chen, <i>University of Science and Technology of China and Nanyang Technological University</i> ; Shengjian Guo, <i>Baidu Security</i> ; Yinxiang Xue, <i>University of Science and Technology of China</i> ; Yulei Sui, <i>University of Technology Sydney</i> ; Cen Zhang and Yuekang Li, <i>Nanyang Technological University</i> ; Haijun Wang, <i>Ant Financial Services Group</i> ; Yang Liu, <i>Nanyang Technological University</i> | |
| Mobile 2 and Malware | |
| On Training Robust PDF Malware Classifiers | 2343 |
| Yizheng Chen, Shiqi Wang, Dongdong She, and Suman Jana, <i>Columbia University</i> | |
| Measuring and Modeling the Label Dynamics of Online Anti-Malware Engines. | 2361 |
| Shuofei Zhu, <i>The Pennsylvania State University</i> ; Jianjun Shi, <i>BIT, The Pennsylvania State University</i> ; Limin Yang, <i>University of Illinois at Urbana-Champaign</i> ; Boqin Qin, <i>BUPT, The Pennsylvania State University</i> ; Ziyi Zhang, <i>USTC, The Pennsylvania State University</i> ; Linhai Song, <i>Pennsylvania State University</i> ; Gang Wang, <i>University of Illinois at Urbana-Champaign</i> | |
| FIRMSCOPE: Automatic Uncovering of Privilege-Escalation Vulnerabilities in Pre-Installed Apps in Android Firmware | 2379 |
| Mohamed Elsabagh, Ryan Johnson, and Angelos Stavrou, <i>Kryptowire</i> ; Chaoshun Zuo, Qingchuan Zhao, and Zhiqiang Lin, <i>The Ohio State University</i> | |
| Automatic Hot Patch Generation for Android Kernels | 2397 |
| Zhengzi Xu, <i>Nanyang Technological University</i> ; Yulong Zhang, Longri Zheng, Liangzhao Xia, and Chenfu Bao, <i>Baidu X-Lab</i> ; Zhi Wang, <i>Florida State University</i> ; Yang Liu, <i>Nanyang Technological University</i> | |
| iOS, Your OS, Everybody’s OS: Vetting and Analyzing Network Services of iOS Applications | 2415 |
| Zhushou Tang, <i>Shanghai Jiao Tong University and PWNZEN InfoTech Co., LTD</i> ; Ke Tang, <i>Shanghai Jiao Tong University</i> ; Minhui Xue, <i>The University of Adelaide</i> ; Yuan Tian, <i>University of Virginia</i> ; Sen Chen, <i>Nanyang Technological University</i> ; Muhammad Ikram, <i>Macquarie University</i> ; Tielei Wang, <i>PWNZEN InfoTech Co., LTD</i> ; Haojin Zhu, <i>Shanghai Jiao Tong University</i> | |
| Data Security/Secure Computation | |
| SEAL: Attack Mitigation for Encrypted Databases via Adjustable Leakage | 2433 |
| Ioannis Demertzis, <i>University of Maryland</i> ; Dimitrios Papadopoulos, <i>Hong Kong University of Science and Technology</i> ; Charalampos Papamanthou, <i>University of Maryland</i> ; Saurabh Shintre, <i>NortonLifeLock Research Group</i> | |

PANCAKE: Frequency Smoothing for Encrypted Data Stores 2451
Paul Grubbs, *Cornell Tech*; Anurag Khandelwal, *Yale University*; Marie-Sarah Lacharité, *Royal Holloway, University of London*; Lloyd Brown, *University of California, Berkeley*; Lucy Li, *Cornell Tech*; Rachit Agarwal, *Cornell University*; Thomas Ristenpart, *Cornell Tech*

Droplet: Decentralized Authorization and Access Control for Encrypted Data Streams 2469
Hossein Shafagh and Lukas Burkhalter, *ETH Zurich*; Sylvia Ratnasamy, *UC Berkeley*; Anwar Hithnawi, *ETH Zurich & UC Berkeley*

Secure parallel computation on national scale volumes of data 2487
Sahar Mazloom and Phi Hung Le, *George Mason University*; Samuel Ranellucci, *Unbound Tech*; S. Dov Gordon, *George Mason University*

DELPHI: A Cryptographic Inference Service for Neural Networks 2505
Pratyush Mishra, Ryan Lehmkuhl, Akshayaram Srinivasan, Wenting Zheng, and Raluca Ada Popa, *UC Berkeley*

Fuzzing 2

Analysis of DTLS Implementations Using Protocol State Fuzzing 2523
Paul Fiterau-Brosteau and Bengt Jonsson, *Uppsala University*; Robert Merget, *Ruhr-University Bochum*; Joeri de Ruiter, *SIDN Labs*; Konstantinos Sagonas, *Uppsala University*; Juraj Somorovsky, *Paderborn University*

Agamoto: Accelerating Kernel Driver Fuzzing with Lightweight Virtual Machine Checkpoints 2541
Dokyung Song, *University of California, Irvine*; Felicitas Hetzelt, *Technische Universität Berlin*; Jonghwan Kim and Brent Byunghoon Kang, *KAIST*; Jean-Pierre Seifert, *Technische Universität Berlin*; Michael Franz, *University of California, Irvine*

USBfuzz: A Framework for Fuzzing USB Drivers by Device Emulation 2559
Hui Peng, *Purdue University*; Mathias Payer, *EPFL*

GREYONE: Data Flow Sensitive Fuzzing 2577
Shuitao Gan, *State Key Laboratory of Mathematical Engineering and Advanced Computing*; Chao Zhang, *Institute for Network Sciences and Cyberspace of Tsinghua University*; Beijing National Research Center for Information Science and Technology; Peng Chen, *ByteDance Inc.*; Bodong Zhao, *Institute for Network Science and Cyberspace, Tsinghua University*; Xiaojun Qin and Dong Wu, *State Key Laboratory of Mathematical Engineering and Advanced Computing*; Zuoning Chen, *National Research Center of Parallel Computer Engineering and Technology*

Fuzzing Error Handling Code using Context-Sensitive Software Fault Injection 2595
Zu-Ming Jiang and Jia-Ju Bai, *Tsinghua University*; Kangjie Lu, *University of Minnesota*; Shi-Min Hu, *Tsinghua University*

Montage: A Neural Network Language Model-Guided JavaScript Engine Fuzzer 2613
Suyoung Lee, HyungSeok Han, Sang Kil Cha, and Soeul Son, *KAIST*

Voice and Speech

Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems 2631
Takeshi Sugawara, *The University of Electro-Communications*; Benjamin Cyr, Sara Rampazzi, Daniel Genkin, and Kevin Fu, *University of Michigan*

SkillExplorer: Understanding the Behavior of Skills in Large Scale 2649
Zhixiu Guo, Zijin Lin, Pan Li, and Kai Chen, *SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, China*; School of Cyber Security, *University of Chinese Academy of Sciences, China*

Devil's Whisper: A General Approach for Physical Adversarial Attacks against Commercial Black-box Speech Recognition Devices 2667
Yuxuan Chen, *SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences*; School of Cyber Security, *University of Chinese Academy of Sciences*; Department of Computer Science, *Florida Institute of Technology*; Xuejing Yuan, Jiangshan Zhang, and Yue Zhao, *SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences*; School of Cyber Security, *University of Chinese Academy of Sciences*; Shengzhi Zhang, Department of Computer Science, *Metropolitan College, Boston University, USA*; Kai Chen, *SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences*; School of Cyber Security, *University of Chinese Academy of Sciences*; XiaoFeng Wang, *School of Informatics and Computing, Indiana University Bloomington*

Void: A fast and light voice liveness detection system 2685
Muhammad Ejaz Ahmed, *Data61, CSIRO*; Il-Youp Kwak, *Chung-Ang University*; Jun Ho Huh and Iljoo Kim, *Samsung Research*; Taekkyung Oh, *KAIST and Sungkyunkwan University*; Hyounghick Kim, *Sungkyunkwan University*

Preech: A System for Privacy-Preserving Speech Transcription 2703
Shimaa Ahmed, Amrita Roy Chowdhury, and Kassem Fawaz, and Parmesh Ramanathan, *University of Wisconsin—Madison*

Blockchains

BlockSci: Design and applications of a blockchain analysis platform 2721
Harry Kalodner, Malte Möser, and Kevin Lee, *Princeton University*; Steven Goldfeder, *Cornell Tech*; Martin Plattner, *University of Innsbruck*; Alishah Chator, *Johns Hopkins University*; Arvind Narayanan, *Princeton University*

Remote Side-Channel Attacks on Anonymous Transactions 2739
Florian Tramer and Dan Boneh, *Stanford University*; Kenny Paterson, *ETH Zurich*

ETHBMC: A Bounded Model Checker for Smart Contracts 2757
Joel Frank, Cornelius Aschermann, and Thorsten Holz, *Ruhr-University Bochum*

TxSPECTOR: Uncovering Attacks in Ethereum from Transactions 2775
Mengya Zhang, Xiaokuan Zhang, Yinqian Zhang, and Zhiqiang Lin, *The Ohio State University*

An Ever-evolving Game: Evaluation of Real-world Attacks and Defenses in Ethereum Ecosystem 2793
Shunfan Zhou, Zheming Yang, and Jie Xiang, *Fudan University*; Yinzhi Cao, *Johns Hopkins University*; Min Yang and Yuan Zhang, *Fudan University*