# 31st USENIX Security Symposium (USENIX Security'22)

Boston, Massachusetts, USA
10-12 August 2022

Volume 1 of 6

ISBN: 978-1-7138-6075-4

**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© (2022) by Usenix Association
All rights reserved.

Printed with permission by Curran Associates, Inc. (2022)

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

# 31st USENIX Security Symposium

## August 10–12, 2022
## Boston, MA, USA

## Wednesday, August 10

### Measurement I: Network

**Under the Hood of DANE Mismanagement in SMTP** .... 1
Hyeonmin Lee, *Seoul National University;* Md. Ishtiaq Ashiq, *Virginia Tech;* Moritz Müller, *SIDN Labs;* Roland van Rijswijk-Deij, *University of Twente & NLnet Labs;* Taekyoung “Ted” Kwon, *Seoul National University;* Taejoong Chung, *Virginia Tech*

**Seeing the Forest for the Trees: Understanding Security Hazards in the 3GPP Ecosystem through Intelligent Analysis on Change Requests** .... 17
Yi Chen and Di Tang, *Indiana University Bloomington;* Yepeng Yao, *{CAS-KLONAT, BKLONSPT}, Institute of Information Engineering, CAS, and School of Cyber Security, University of Chinese Academy of Sciences;* Mingming Zha and XiaoFeng Wang, *Indiana University Bloomington;* Xiaozhong Liu, *Worcester Polytechnic Institute;* Haixu Tang and Dongfang Zhao, *Indiana University Bloomington*

**Exploring the Unchartered Space of Container Registry Typosquatting** .... 35
Guannan Liu, *Virginia Tech;* Xing Gao, *University of Delaware;* Haining Wang, *Virginia Tech;* Kun Sun, *George Mason University*

**Uninvited Guests: Analyzing the Identity and Behavior of Certificate Transparency Bots** .... 53
Brian Kondracki, Johnny So, and Nick Nikiforakis, *Stony Brook University*

### Kernel Security

**Playing for K(H)eaps: Understanding and Improving Linux Kernel Exploit Reliability** .... 71
Kyle Zeng, *Arizona State University;* Yueqi Chen, *Pennsylvania State University;* Haehyun Cho, *Arizona State University and Soongsil University;* Xinyu Xing, *Pennsylvania State University;* Adam Doupé, Yan Shoshitaishvili, and Tiffany Bao, *Arizona State University*

**In-Kernel Control-Flow Integrity on Commodity OSes using ARM Pointer Authentication** .... 89
Sungbae Yoo, Jinbum Park, Seolheui Kim, and Yeji Kim, *Samsung Research;* Taesoo Kim, *Samsung Research and Georgia Institute of Technology*

**Midas: Systematic Kernel TOCTTOU Protection** .... 107
Atri Bhattacharyya, *EPFL;* Uros Tesic, *Nvidia;* Mathias Payer, *EPFL*

**LinKRID: Vetting Imbalance Reference Counting in Linux kernel with Symbolic Execution** .... 125
Jian Liu, *{CAS-KLONAT, BKLONSPT}, Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences;* Lin Yi, *{CAS-KLONAT, BKLONSPT}, Institute of Information Engineering, Chinese Academy of Sciences;* Weiteng Chen, Chengyu Song, and Zhiyun Qian, *UC Riverside;* Qiuping Yi, *Beijing University of Posts and Telecommunications and Beijing Key Lab of Intelligent Telecommunication Software and Multimedia*

### Web Security I: Vulnerabilities

**Mining Node.js Vulnerabilities via Object Dependence Graph and Query** .... 143
Song Li and Mingqing Kang, *Johns Hopkins University;* Jianwei Hou, *Johns Hopkins University/Renmin University of China;* Yinzhi Cao, *Johns Hopkins University*

**Mistrust Plugins You Must: A Large-Scale Study Of Malicious Plugins In WordPress Marketplaces** .... 161
Ranjita Pai Kasturi, Jonathan Fuller, Yiting Sun, Omar Chabklo, Andres Rodriguez, Jeman Park, and Brendan Saltaformaggio, *Georgia Institute of Technology*

**Web Cache Deception Escalates!** .... 179
Seyed Ali Mirheidari, *University of Trento & Splunk Inc.;* Matteo Golinelli, *University of Trento;* Kaan Onarlioglu, *Akamai Technologies;* Engin Kirda, *Northeastern University;* Bruno Crispo, *University of Trento*

**FUGIO: Automatic Exploit Generation for PHP Object Injection Vulnerabilities** . . . . . . . . . . . . . . . . . . . . . . . . . . . **197**
Sunnyeo Park and Daejun Kim, *KAIST;* Suman Jana, *Columbia University;* Sooel Son, *KAIST*

## Crypto I: Attacking Implementations

**TLS-Anvil: Adapting Combinatorial Testing for TLS Libraries** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **215**
Marcel Maehren and Philipp Nieting, *Ruhr University Bochum;* Sven Hebrok, *Paderborn University;* Robert Merget, *Ruhr University Bochum;* Juraj Somorovsky, *Paderborn University;* Jörg Schwenk, *Ruhr University Bochum*

**Open to a fault: On the passive compromise of TLS keys via transient errors** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **233**
George Arnold Sullivan, *University of California, San Diego;* Jackson Sippe, *University of Colorado Boulder;* Nadia Heninger, *University of California, San Diego;* Eric Wustrow, *University of Colorado Boulder*

**Trust Dies in Darkness: Shedding Light on Samsung's TrustZone Keymaster Design** . . . . . . . . . . . . . . . . . . . . . . . **251**
Alon Shakevsky, Eyal Ronen, and Avishai Wool, *Tel-Aviv University*

**Breaking Bridgefy, again: Adopting libsignal is not enough** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **269**
Martin R. Albrecht, *Information Security Group, Royal Holloway, University of London;* Raphael Eikenberg and Kenneth G. Paterson, *Applied Cryptography Group, ETH Zurich*

## User Studies I: At-Risk Users

**"I feel invaded, annoyed, anxious and I may protect myself": Individuals' Feelings about Online Tracking and their Protective Behaviour across Gender and Country** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **287**
Kovila P.L. Coopamootoo and Maryam Mehrnezhad, *Newcastle University;* Ehsan Toreini, *Durham University*

**"Like Lesbians Walking the Perimeter": Experiences of U.S. LGBTQ+ Folks With Online Security, Safety, and Privacy Advice** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **305**
Christine Geeng and Mike Harris, *University of Washington;* Elissa Redmiles, *Max Planck Institute for Software Systems;* Franziska Roesner, *University of Washington*

**"They Look at Vulnerability and Use That to Abuse You": Participatory Threat Modelling with Migrant Domestic Workers** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **323**
Julia Słupska and Selina Cho, *University of Oxford;* Marissa Begonia, *Voice of Domestic Workers;* Ruba Abu-Salma, *King's College London;* Nayanatara Prakash, *University of Oxford;* Mallika Balakrishnan, *Migrants Organise*

**Networks of Care: Tech Abuse Advocates' Digital Security Practices** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **341**
Julia Slupska, *University of Oxford;* Angelika Strohmayer, *Northumbria University*

## Software Vulnerabilities

**How Long Do Vulnerabilities Live in the Code? A Large-Scale Empirical Measurement Study on FOSS Vulnerability Lifetimes** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **359**
Nikolaos Alexopoulos, Manuel Brack, Jan Philipp Wagner, Tim Grube, and Max Mühlhäuser, *Technical University of Darmstadt*

**Expected Exploitability: Predicting the Development of Functional Vulnerability Exploits** . . . . . . . . . . . . . . . . . . . . **377**
Octavian Suciu, *University of Maryland, College Park;* Connor Nelson, Zhuoer Lyu, and Tiffany Bao, *Arizona State University;* Tudor Dumitraş, *University of Maryland, College Park*

**OS-Aware Vulnerability Prioritization via Differential Severity Analysis** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **395**
Qiushi Wu, *University of Minnesota;* Yue Xiao and Xiaojing Liao, *Indiana University Bloomington;* Kangjie Lu, *University of Minnesota*

**Arbiter: Bridging the Static and Dynamic Divide in Vulnerability Discovery on Binary Programs** . . . . . . . . . . . . . **413**
Jayakrishna Vadayath, *Arizona State University;* Moritz Eckert, *EURECOM;* Kyle Zeng, *Arizona State University;* Nicolaas Weideman, *University of Southern California;* Gokulkrishna Praveen Menon, *Arizona State University;* Yanick Fratantonio, *Cisco Systems Inc.;* Davide Balzarotti, *EURECOM;* Adam Doupé, Tiffany Bao, and Ruoyu Wang, *Arizona State University;* Christophe Hauser, *University of Southern California;* Yan Shoshitaishvili, *Arizona State University*

## Network Security I: Scanning & Censorship

**Spoki: Unveiling a New Wave of Scanners through a Reactive Network Telescope** . . . . . . . . . . . . . . . . . . . . . . . . . . **431**
Raphael Hiesgen, *HAW Hamburg;* Marcin Nawrocki, *Freie Universität Berlin;* Alistair King, *Kentik;* Alberto Dainotti, *CAIDA, UC San Diego and Georgia Institute of Technology;* Thomas C. Schmidt, *HAW Hamburg;* Matthias Wählisch, *Freie Universität Berlin*

**Many Roads Lead To Rome: How Packet Headers Influence DNS Censorship Measurement** . . . . . . . . . . . . . . . . . **449**
Abhishek Bhaskar and Paul Pearce, *Georgia Institute of Technology*

**GET /out: Automated Discovery of Application-Layer Censorship Evasion Strategies** . . . . . . . . . . . . . . . . . . . . . . **465**
Michael Harrity, Kevin Bock, Frederick Sell, and Dave Levin, *University of Maryland*

**OpenVPN is Open to VPN Fingerprinting** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **483**
Diwen Xue, Reethika Ramesh, and Arham Jain, *University of Michigan;* Michalis Kallitsis, *Merit Network, Inc.;* J. Alex Halderman, *University of Michigan;* Jedidiah R. Crandall, *Arizona State University/Breakpointing Bad;* Roya Ensafi, *University of Michigan*

## Differential Privacy

**Pool Inference Attacks on Local Differential Privacy: Quantifying the Privacy Guarantees of Apple's Count Mean Sketch in Practice** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **501**
Andrea Gadotti, *Imperial College London;* Florimond Houssiau, *Alan Turing Institute;* Meenatchi Sundaram Muthu Selva Annamalai and Yves-Alexandre de Montjoye, *Imperial College London*

**Poisoning Attacks to Local Differential Privacy Protocols for Key-Value Data** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **519**
Yongji Wu, Xiaoyu Cao, Jinyuan Jia, and Neil Zhenqiang Gong, *Duke University*

**Communication-Efficient Triangle Counting under Local Differential Privacy** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **537**
Jacob Imola, *UC San Diego;* Takao Murakami, *AIST;* Kamalika Chaudhuri, *UC San Diego*

**Twilight: A Differentially Private Payment Channel Network** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **555**
Maya Dotan, Saar Tochner, Aviv Zohar, and Yossi Gilad, *The Hebrew University of Jerusalem*

## Measurement II: Auditing & Best Practices

**Watching the watchers: bias and vulnerability in remote proctoring software** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **571**
Ben Burgess, *Princeton University;* Avi Ginsberg, *Georgetown Law;* Edward W. Felten, *Princeton University;* Shaanan Cohney, *University of Melbourne*

**The Antrim County 2020 Election Incident: An Independent Forensic Investigation** . . . . . . . . . . . . . . . . . . . . . . . . **589**
J. Alex Halderman, *University of Michigan*

**An Audit of Facebook's Political Ad Policy Enforcement** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **607**
Victor Le Pochat, *imec-DistriNet, KU Leuven;* Laura Edelson, *New York University;* Tom Van Goethem and Wouter Joosen, *imec-DistriNet, KU Leuven;* Damon McCoy and Tobias Lauinger, *New York University*

**Building an Open, Robust, and Stable Voting-Based Domain Top List** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **625**
Qinge Xie, *Georgia Institute of Technology;* Shujun Tang, *QI-ANXIN Technology Research Institute;* Xiaofeng Zheng, *QI-ANXIN Technology Research Institute and Tsinghua University;* Qingran Lin, *QI-ANXIN Technology Research Institute;* Baojun Liu, *Tsinghua University;* Haixin Duan, *QI-ANXIN Technology Research Institute and Tsinghua University;* Frank Li, *Georgia Institute of Technology*

## Side Channels I: Hardware

**AMD Prefetch Attacks through Power and Time** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **643**
Moritz Lipp and Daniel Gruss, *Graz University of Technology;* Michael Schwarz, *CISPA Helmholtz Center for Information Security*

**Hiding in Plain Sight? On the Efficacy of Power Side Channel-Based Control Flow Monitoring** . . . . . . . . . . . . . . . . **661**
Yi Han, Matthew Chan, and Zahra Aref, *Rutgers University;* Nils Ole Tippenhauer, *CISPA Helmholtz Center for Information Security;* Saman Zonouz, *Georgia Tech*

**Hertzbleed: Turning Power Side-Channel Attacks Into Remote Timing Attacks on x86** ........ **679**
Yingchen Wang, *University of Texas at Austin;* Riccardo Paccagnella and Elizabeth Tang He, *University of Illinois Urbana-Champaign;* Hovav Shacham, *University of Texas at Austin;* Christopher W. Fletcher, *University of Illinois Urbana-Champaign;* David Kohlbrenner, *University of Washington*

**Binoculars: Contention-Based Side-Channel Attacks Exploiting the Page Walker** ........ **699**
Zirui Neil Zhao, *University of Illinois Urbana-Champaign;* Adam Morrison, *Tel Aviv University;* Christopher W. Fletcher and Josep Torrellas, *University of Illinois Urbana-Champaign*

## Web Security II: Fingerprinting

**The Dangers of Human Touch: Fingerprinting Browser Extensions through User Actions** ........ **717**
Konstantinos Solomos, Panagiotis Ilia, and Soroush Karami, *University of Illinois at Chicago;* Nick Nikiforakis, *Stony Brook University;* Jason Polakis, *University of Illinois at Chicago*

**Unleash the *Simulacrum*: Shifting Browser Realities for Robust Extension-Fingerprinting Prevention** ........ **735**
Soroush Karami, *University of Illinois at Chicago;* Faezeh Kalantari, Mehrnoosh Zaeifi, Xavier J. Maso, and Erik Trickel, *Arizona State University;* Panagiotis Ilia, *University of Illinois at Chicago;* Yan Shoshitaishvili and Adam Doupé, *Arizona State University;* Jason Polakis, *University of Illinois at Chicago*

**Online Website Fingerprinting: Evaluating Website Fingerprinting Attacks on Tor in the Real World** ........ **753**
Giovanni Cherubin, *Alan Turing Institute;* Rob Jansen, *U.S. Naval Research Laboratory;* Carmela Troncoso, *EPFL SPRING Lab*

**QCSD: A QUIC Client-Side Website-Fingerprinting Defence Framework** ........ **771**
Jean-Pierre Smith and Luca Dolfi, *ETH Zurich;* Prateek Mittal, *Princeton University;* Adrian Perrig, *ETH Zurich*

## Crypto II: Performance Improvements

**Secure Poisson Regression** ........ **791**
Mahimna Kelkar, *Cornell Tech;* Phi Hung Le, Mariana Raykova, and Karn Seth, *Google*

**Cheetah: Lean and Fast Secure Two-Party Deep Neural Network Inference** ........ **809**
Zhicong Huang, Wen-jie Lu, Cheng Hong, and Jiansheng Ding, *Alibaba Group*

**Piranha: A GPU Platform for Secure Computation** ........ **827**
Jean-Luc Watson, Sameer Wagh, and Raluca Ada Popa, *University of California, Berkeley*

**OpenSSLNTRU: Faster post-quantum TLS key exchange** ........ **845**
Daniel J. Bernstein, *University of Illinois at Chicago and Ruhr University Bochum;* Billy Bob Brumley, *Tampere University;* Ming-Shing Chen, *Ruhr University Bochum;* Nicola Tuveri, *Tampere University*

## User Studies II: Sharing

**How Are Your Zombie Accounts? Understanding Users' Practices and Expectations on Mobile App Account Deletion** ........ **863**
Yijing Liu, Yan Jia, Qingyin Tan, and Zheli Liu, *Nankai University;* Luyi Xing, *Indiana University Bloomington*

**"How Do You Not Lose Friends?": Synthesizing a Design Space of Social Controls for Securing Shared Digital Resources Via Participatory Design Jams** ........ **881**
Eyitemi Moju-Igbene, Hanan Abdi, Alan Lu, and Sauvik Das, *Georgia Institute of Technology*

**Caring about Sharing: User Perceptions of Multiparty Data Sharing** ........ **899**
Bailey Kacsmar, Kyle Tilbury, Miti Mazmudar, and Florian Kerschbaum, *University of Waterloo*

**Neither Access nor Control: A Longitudinal Investigation of the Efficacy of User Access-Control Solutions on Smartphones** ........ **917**
Masoud Mehrabi Koushki, Yue Huang, Julia Rubin, and Konstantin Beznosov, *University of British Columbia*

## Hardware Security I: Attacks & Defenses

**Jenny: Securing Syscalls for PKU-based Memory Isolation Systems** ........ **935**
David Schrammel, Samuel Weiser, Richard Sadek, and Stefan Mangard, *Graz University of Technology*

**Physical-Layer Attacks Against Pulse Width Modulation-Controlled Actuators** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **953**
Gökçen Yılmaz Dayanıklı, *Qualcomm;* Sourav Sinha, *Virginia Tech;* Devaprakash Muniraj, *IIT Madras;*
Ryan M. Gerdes and Mazen Farhood, *Virginia Tech;* Mani Mina, *Iowa State University*

**Branch History Injection: On the Effectiveness of Hardware Mitigations Against Cross-Privilege Spectre-v2 Attacks** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **971**
Enrico Barberis, Pietro Frigo, Marius Muench, Herbert Bos, and Cristiano Giuffrida, *Vrije Universiteit Amsterdam*

**TLB;DR: Enhancing TLB-based Attacks with TLB Desynchronized Reverse Engineering** . . . . . . . . . . . . . . . . . . . . **989**
Andrei Tatar, *Vrije Universiteit, Amsterdam;* Daniël Trujillo, *Vrije Universiteit, Amsterdam, and ETH Zurich;*
Cristiano Giuffrida and Herbert Bos, *Vrije Universiteit, Amsterdam*

## Fuzzing I: Networks

**FuzzOrigin: Detecting UXSS vulnerabilities in Browsers through Origin Fuzzing** . . . . . . . . . . . . . . . . . . . . . . . . . . **1007**
Sunwoo Kim, *Samsung Research;* Young Min Kim, Jaewon Hur, and Suhwan Song, *Seoul National University;*
Gwangmu Lee, *EPFL;* Byoungyoung Lee, *Seoul National University*

**BrakTooth: Causing Havoc on Bluetooth Link Manager via Directed Fuzzing** . . . . . . . . . . . . . . . . . . . . . . . . . . . . **1025**
Matheus E. Garbelini, Vaibhav Bedi, and Sudipta Chattopadhyay, *Singapore University of Technology and Design;*
Sumei Sun and Ernest Kurniawan, *Institute for Infocomm Research, A*Star*

**AmpFuzz: Fuzzing for Amplification DDoS Vulnerabilities** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **1043**
Johannes Krupp, *CISPA Helmholtz Center for Information Security;* Ilya Grishchenko, *University of California, Santa Barbara;* Christian Rossow, *CISPA Helmholtz Center for Information Security*

**Frameshifter: Security Implications of HTTP/2-to-HTTP/1 Conversion Anomalies** . . . . . . . . . . . . . . . . . . . . . . . . . .**1061**
Bahruz Jabiyev, Steven Sprecher, Anthony Gavazzi, and Tommaso Innocenti, *Northeastern University;* Kaan Onarlioglu, *Akamai Technologies;* Engin Kirda, *Northeastern University*

## Smart Homes I

**Your Microphone Array Retains Your Identity: A Robust Voice Liveness Detection System for Smart Speakers** . . **1077**
Yan Meng and Jiachun Li, *Shanghai Jiao Tong University;* Matthew Pillari, Arjun Deopujari, Liam Brennan, and
Hafsah Shamsie, *University of Virginia;* Haojin Zhu, *Shanghai Jiao Tong University;* Yuan Tian, *University of Virginia*

**Lumos: Identifying and Localizing Diverse Hidden IoT Devices in an Unfamiliar Environment** . . . . . . . . . . . . . . . **1095**
Rahul Anand Sharma, Elahe Soltanaghaei, Anthony Rowe, and Vyas Sekar, *Carnegie Mellon University*

**SkillDetective: Automated Policy-Violation Detection of Voice Assistant Applications in the Wild** . . . . . . . . . . . . . **1113**
Jeffrey Young, Song Liao, and Long Cheng, *Clemson University;* Hongxin Hu, *University at Buffalo;* Huixing Deng, *Clemson University*

**"OK, Siri" or "Hey, Google": Evaluating Voiceprint Distinctiveness via Content-based PROLE Score** . . . . . . . . .**1131**
Ruiwen He, Xiaoyu Ji, and Xinfeng Li, *Zhejiang University;* Yushi Cheng, *Tsinghua University;* Wenyuan Xu, *Zhejiang University*

## Measurement III

**Helping hands: Measuring the impact of a large threat intelligence sharing community** . . . . . . . . . . . . . . . . . . . . . .**1149**
Xander Bouwman, *Delft University of Technology;* Victor Le Pochat, *imec-DistriNet, KU Leuven;* Pawel Foremski, *Farsight Security, Inc. / IITiS PAN;* Tom Van Goethem, *imec-DistriNet, KU Leuven;* Carlos H. Gañán, *Delft University of Technology and ICANN;* Giovane C. M. Moura, *SIDN Labs;* Samaneh Tajalizadehkhoob, *ICANN;* Wouter Joosen, *imec-DistriNet, KU Leuven;* Michel van Eeten, *Delft University of Technology*

**A Large-scale Temporal Measurement of Android Malicious Apps: Persistence, Migration, and Lessons Learned** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .**1167**
Yun Shen and Pierre-Antoine Vervier, *Norton Research Group;* Gianluca Stringhini, *Boston University*

**A Large-scale and Longitudinal Measurement Study of DKIM Deployment** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **1185**
Chuhan Wang, Kaiwen Shen, and Minglei Guo, *Tsinghua University;* Yuxuan Zhao, *North China Institute of Computing Technology;* Mingming Zhang, Jianjun Chen, and Baojun Liu, *Tsinghua University;* Xiaofeng Zheng and Haixin Duan, *Tsinghua University and Qi An Xin Technology Research Institute;* Yanzhong Lin and Qingfeng Pan, *Coremail Technology Co. Ltd*

**A Large-scale Investigation into Geodifferences in Mobile Apps** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **1203**
Renuka Kumar, Apurva Virkud, Ram Sundara Raman, Atul Prakash, and Roya Ensafi, *University of Michigan*

## Fuzzing II: Low-Level

**Morphuzz: Bending (Input) Space to Fuzz Virtual Devices** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **1221**
Alexander Bulekov, *Boston University and Red Hat;* Bandan Das and Stefan Hajnoczi, *Red Hat;* Manuel Egele, *Boston University*

**Fuzzware: Using Precise MMIO Modeling for Effective Firmware Fuzzing** . . . . . . . . . . . . . . . . . . . . . . . . . . . . **1239**
Tobias Scharnowski, Nils Bars, and Moritz Schloegel, *Ruhr-Universität Bochum;* Eric Gustafson, *UC Santa Barbara;* Marius Muench, *Vrije Universiteit Amsterdam;* Giovanni Vigna, *UC Santa Barbara and VMware;* Christopher Kruegel, *UC Santa Barbara;* Thorsten Holz and Ali Abbasi, *Ruhr-Universität Bochum*

**MundoFuzz: Hypervisor Fuzzing with Statistical Coverage Testing and Grammar Inference** . . . . . . . . . . . . . . . . **1257**
Cheolwoo Myung, Gwangmu Lee, and Byoungyoung Lee, *Seoul National University*

**Drifuzz: Harvesting Bugs in Device Drivers from Golden Seeds** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **1275**
Zekun Shen, Ritik Roongta, and Brendan Dolan-Gavitt, *NYU*

## Wireless Security

**LTrack: Stealthy Tracking of Mobile Phones in LTE** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **1291**
Martin Kotuliak, Simon Erni, Patrick Leu, Marc Röschlin, and Srdjan Čapkun, *ETH Zurich*

**Watching the Watchers: Practical Video Identification Attack in LTE Networks** . . . . . . . . . . . . . . . . . . . . . . . . . **1307**
Sangwook Bae, Mincheol Son, Dongkwan Kim, CheolJun Park, Jiho Lee, Sooel Son, and Yongdae Kim, *Korea Advanced Institute of Science and Technology* (*KAIST*)

**DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices** . . . . . . . . . . . . . . . . . . . . . . . . . . . . **1325**
CheolJun Park, Sangwook Bae, BeomSeok Oh, Jiho Lee, Eunkyu Lee, Insu Yun, and Yongdae Kim, *Korea Advanced Institute of Science and Technology* (*KAIST*)

**Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging** . . . . . . . . . . . . . . . . . . . . . . . . . . **1343**
Patrick Leu and Giovanni Camurati, *ETH Zurich;* Alexander Heinrich, *TU Darmstadt;* Marc Roeschlin and Claudio Anliker, *ETH Zurich;* Matthias Hollick, *TU Darmstadt;* Srdjan Capkun, *ETH Zurich;* Jiska Classen, *TU Darmstadt*

## ML I: Federated Learning

**Simc: ML Inference Secure Against Malicious Clients at Semi-Honest Cost** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **1361**
Nishanth Chandran, Divya Gupta, and Sai Lakshmi Bhavana Obbattu, *Microsoft Research;* Akash Shah, *UCLA*

**Efficient Differentially Private Secure Aggregation for Federated Learning via Hardness of Learning with Errors** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **1379**
Timothy Stevens, Christian Skalka, and Christelle Vincent, *University of Vermont;* John Ring, *MassMutual;* Samuel Clark, *Raytheon;* Joseph Near, *University of Vermont*

**Label Inference Attacks Against Vertical Federated Learning** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **1397**
Chong Fu, *Zhejiang University;* Xuhong Zhang and Shouling Ji, *Binjiang Institute of Zhejiang University;* Jinyin Chen, *Zhejiang University of Technology;* Jingzheng Wu, *Institute of Software, Chinese Academy of Sciences;* Shanqing Guo, *Shandong University;* Jun Zhou and Alex X. Liu, *Ant Group;* Ting Wang, *Pennsylvania State University*

**FLAME: Taming Backdoors in Federated Learning** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .**1415**
Thien Duc Nguyen and Phillip Rieger, *Technical University of Darmstadt;* Huili Chen, *University of California San Diego;* Hossein Yalame, Helen Möllering, and Hossein Fereidooni, *Technical University of Darmstadt;* Samuel Marchal, *Aalto University and F-Secure;* Markus Miettinen, *Technical University of Darmstadt;* Azalia Mirhoseini, *Google;* Shaza Zeitouni, *Technical University of Darmstadt;* Farinaz Koushanfar, *University of California San Diego;* Ahmad-Reza Sadeghi and Thomas Schneider, *Technical University of Darmstadt*

# Thursday, August 11

## Deanonymization

**Mitigating Membership Inference Attacks by Self-Distillation Through a Novel Ensemble Architecture** ........ **1433**
Xinyu Tang, Saeed Mahloujifar, and Liwei Song, *Princeton University;* Virat Shejwalkar, Milad Nasr, and Amir Houmansadr, *University of Massachusetts Amherst;* Prateek Mittal, *Princeton University*

**Synthetic Data – Anonymisation Groundhog Day** ........ **1451**
Theresa Stadler, *EPFL;* Bristena Oprisanu, *UCL;* Carmela Troncoso, *EPFL*

**Attacks on Deidentification's Defenses** ........ **1469**
Aloni Cohen, *University of Chicago*

**Birds of a Feather Flock Together: How Set Bias Helps to Deanonymize You via Revealed Intersection Sizes** .... **1487**
Xiaojie Guo, Ye Han, Zheli Liu, Ding Wang, and Yan Jia, *Nankai University;* Jin Li, *Guangzhou University*

**Targeted Deanonymization via the Cache Side Channel: Attacks and Defenses** ........ **1505**
Mojtaba Zaheri, Yossi Oren, and Reza Curtmola, *New Jersey Institute of Technology*

## Mobile Security

**FReD: Identifying File Re-Delegation in Android System Services** ........ **1525**
Sigmund Albert Gorski III, Seaver Thorn, and William Enck, *North Carolina State University;* Haining Chen, *Google*

**GhostTouch: Targeted Attacks on Touchscreens without Physical Touch** ........ **1543**
Kai Wang, *Zhejiang University;* Richard Mitev, *Technical University of Darmstadt;* Chen Yan and Xiaoyu Ji, *Zhejiang University;* Ahmad-Reza Sadeghi, *Technical University of Darmstadt;* Wenyuan Xu, *Zhejiang University*

**SARA: Secure Android Remote Authorization** ........ **1561**
Abdullah Imran, Habiba Farrukh, Muhammad Ibrahim, Z. Berkay Celik, and Antonio Bianchi, *Purdue University*

**FOAP: Fine-Grained Open-World Android App Fingerprinting** ........ **1579**
Jianfeng Li, Hao Zhou, Shuohan Wu, and Xiapu Luo, *The Hong Kong Polytechnic University;* Ting Wang, *Pennsylvania State University;* Xian Zhan, *The Hong Kong Polytechnic University;* Xiaobo Ma, *Xi'an Jiaotong University*

**Identity Confusion in WebView-based Mobile App-in-app Ecosystems** ........ **1597**
Lei Zhang, Zhibo Zhang, and Ancong Liu, *Fudan University;* Yinzhi Cao, *Johns Hopkins University;* Xiaohan Zhang, Yanjun Chen, Yuan Zhang, Guangliang Yang, and Min Yang, *Fudan University*

## Web Security III: Bots & Authentication

**Automated Detection of Automated Traffic** ........ **1615**
Cormac Herley, *Microsoft Research*

**Inferring Phishing Intention via Webpage Appearance and Dynamics: A Deep Vision Based Approach** ........ **1633**
Ruofan Liu, Yun Lin, Xianglin Yang, and Siang Hwee Ng, *National University of Singapore;* Dinil Mon Divakaran, *Trustwave;* Jin Song Dong, *National University of Singapore*

**Phish in Sheep's Clothing: Exploring the Authentication Pitfalls of Browser Fingerprinting** ........ **1651**
Xu Lin, Panagiotis Ilia, Saumya Solanki, and Jason Polakis, *University of Illinois at Chicago*

**DeepPhish: Understanding User Trust Towards Artificially Generated Profiles in Online Social Networks** ..... **1669**
Jaron Mink, Licheng Luo, and Natã M. Barbosa, *University of Illinois at Urbana-Champaign;* Olivia Figueira, *Santa Clara University;* Yang Wang and Gang Wang, *University of Illinois at Urbana-Champaign*

**Hand Me Your PIN! Inferring ATM PINs of Users Typing with a Covered Hand** ........ **1687**
Matteo Cardaioli, Stefano Cecconello, Mauro Conti, and Simone Milani, *University of Padua;* Stjepan Picek, *Delft University of Technology;* Eugen Saraci, *University of Padua*

## Crypto III: Private Matching & Lookups

**Estimating Incidental Collection in Foreign Intelligence Surveillance: Large-Scale Multiparty Private Set Intersection with Union and Sum** ........ **1705**
Anunay Kulshrestha and Jonathan Mayer, *Princeton University*

**Constant-weight PIR: Single-round Keyword PIR via Constant-weight Equality Operators** . . . . . . . . . . . . . . . . . . .1723
Rasoul Akhavan Mahdavi and Florian Kerschbaum, *University of Waterloo*

**Incremental Offline/Online PIR** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .1741
Yiping Ma and Ke Zhong, *University of Pennsylvania;* Tal Rabin, *University of Pennsylvania and Algorand Foundation;* Sebastian Angel, *University of Pennsylvania and Microsoft Research*

**GPU-accelerated PIR with Client-Independent Preprocessing for Large-Scale Applications** . . . . . . . . . . . . . . . . . . .1759
Daniel Günther and Maurice Heymann, *Technical University of Darmstadt;* Benny Pinkas, *Bar-Ilan University;* Thomas Schneider, *Technical University of Darmstadt*

**Increasing Adversarial Uncertainty to Scale Private Similarity Testing** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .1777
Yiqing Hua and Armin Namavari, *Cornell Tech and Cornell University;* Kaishuo Cheng, *Cornell University;* Mor Naaman and Thomas Ristenpart, *Cornell Tech and Cornell University*

## Passwords

**Pre-hijacked accounts: An Empirical Study of Security Failures in User Account Creation on the Web** . . . . . . . . . .1795
Avinash Sudhodanan, *Independent Researcher;* Andrew Paverd, *Microsoft Security Response Center*

**Leaky Forms: A Study of Email and Password Exfiltration Before Form Submission** . . . . . . . . . . . . . . . . . . . . . . . . 1813
Asuman Senol, *imec-COSIC, KU Leuven;* Gunes Acar, *Radboud University;* Mathias Humbert, *University of Lausanne;* Frederik Zuiderveen Borgesius, *Radboud University*

**Might I Get Pwned: A Second Generation Compromised Credential Checking Service** . . . . . . . . . . . . . . . . . . . . . . 1831
Bijeeta Pal, *Cornell University;* Mazharul Islam, *University of Wisconsin–Madison;* Marina Sanusi Bohuk, *Cornell University;* Nick Sullivan, Luke Valenta, Tara Whalen, and Christopher Wood, *Cloudflare;* Thomas Ristenpart, *Cornell Tech;* Rahul Chatterjee, *University of Wisconsin–Madison*

**Why Users (Don't) Use Password Managers at a Large Educational Institution** . . . . . . . . . . . . . . . . . . . . . . . . . . . 1849
Peter Mayer, *Karlsruhe Institute of Technology;* Collins W. Munyendo, *The George Washington University;* Michelle L. Mazurek, *University of Maryland, College Park;* Adam J. Aviv, *The George Washington University*

**Gossamer: Securely Measuring Password-based Logins** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1867
Marina Sanusi Bohuk, *Cornell University;* Mazharul Islam, *University of Wisconsin–Madison;* Suleman Ahmad, *Cloudflare;* Michael Swift, *University of Wisconsin–Madison;* Thomas Ristenpart, *Cornell Tech;* Rahul Chatterjee, *University of Wisconsin–Madison*

## Smart Vehicles

***DoubleStar*****: Long-Range Attack Towards Depth Estimation based Obstacle Avoidance in Autonomous Systems**. 1885
Ce Zhou, Qiben Yan, and Yan Shi, *Michigan State University;* Lichao Sun, *Lehigh University*

**Security Analysis of Camera-LiDAR Fusion Against Black-Box Attacks on Autonomous Vehicles** . . . . . . . . . . . . . 1903
R. Spencer Hallyburton and Yupei Liu, *Duke University;* Yulong Cao and Z. Morley Mao, *University of Michigan;* Miroslav Pajic, *Duke University*

**SAID: State-aware Defense Against Injection Attacks on In-vehicle Network** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1921
Lei Xue, *The Hong Kong Polytechnic University Shenzhen Research Institute;* Yangyang Liu, Tianqi Li, Kaifa Zhao, Jianfeng Li, Le Yu, and Xiapu Luo, *The Hong Kong Polytechnic University;* Yajin Zhou, *Zhejiang University;* Guofei Gu, *Texas A&M University*

**Towards Automatically Reverse Engineering Vehicle Diagnostic Protocols** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1939
Le Yu, Yangyang Liu, Pengfei Jing, Xiapu Luo, Lei Xue, and Kaifa Zhao, *The Hong Kong Polytechnic University;* Yajin Zhou, *Zhejiang University;* Ting Wang, *The Pennsylvania State University;* Guofei Gu, *Texas A&M University;* Sen Nie and Shi Wu, *Tencent Keen Security Lab*

**Rolling Colors: Adversarial Laser Exploits against Traffic Light Recognition** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1957
Chen Yan, *Zhejiang University;* Zhijian Xu, *Zhejiang University and The Chinese University of Hong Kong;* Zhanyuan Yin, *The University of Chicago;* Xiaoyu Ji and Wenyuan Xu, *Zhejiang University*

## Web Security IV: Defenses

**Provably-Safe Multilingual Software Sandboxing using WebAssembly** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1975
Jay Bosamiya, Wen Shih Lim, and Bryan Parno, *Carnegie Mellon University*

**Backporting Security Patches of Web Applications: A Prototype Design and Implementation on Injection Vulnerability Patches** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1993
Youkun Shi, Yuan Zhang, Tianhan Luo, and Xiangyu Mao, *Fudan University;* Yinzhi Cao, *Johns Hopkins University;* Ziwen Wang, Yudi Zhao, Zongan Huang, and Min Yang, *Fudan University*

**Experimental Security Analysis of the App Model in Business Collaboration Platforms** . . . . . . . . . . . . . . . . . . . . . 2011
Yunang Chen, Yue Gao, Nick Ceccio, Rahul Chatterjee, Kassem Fawaz, and Earlence Fernandes, *University of Wisconsin–Madison*

**SWAPP: A New Programmable Playground for Web Application Security** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2029
Phakpoom Chinprutthiwong, Jianwei Huang, and Guofei Gu, *SUCCESS Lab, Texas A&M University*

**The Security Lottery: Measuring Client-Side Web Security Inconsistencies** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2047
Sebastian Roth, *CISPA Helmholtz Center for Information Security;* Stefano Calzavara, *Università Ca' Foscari Venezia;* Moritz Wilhelm, *CISPA Helmholtz Center for Information Security;* Alvise Rabitti, *Università Ca' Foscari Venezia;* Ben Stock, *CISPA Helmholtz Center for Information Security*

## ML II

**PatchCleanser: Certifiably Robust Defense against Adversarial Patches for Any Image Classifier** . . . . . . . . . . . . . 2065
Chong Xiang, Saeed Mahloujifar, and Prateek Mittal, *Princeton University*

**Transferring Adversarial Robustness Through Robust Representation Matching** . . . . . . . . . . . . . . . . . . . . . . . . . . . 2083
Pratik Vaishnavi, *Stony Brook University;* Kevin Eykholt, *IBM;* Amir Rahmati, *Stony Brook University*

**How Machine Learning Is Solving the Binary Function Similarity Problem** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2099
Andrea Marcelli, Mariano Graziano, Xabier Ugarte-Pedrero, and Yanick Fratantonio, *Cisco Systems, Inc.;* Mohamad Mansouri and Davide Balzarotti, *EURECOM*

**Blacklight: Scalable Defense for Neural Networks against Query-Based Black-Box Attacks** . . . . . . . . . . . . . . . . . . .2117
Huiying Li, Shawn Shan, and Emily Wenger, *University of Chicago;* Jiayun Zhang, *Fudan University;* Haitao Zheng and Ben Y. Zhao, *University of Chicago*

**DnD: A Cross-Architecture Deep Neural Network Decompiler** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2135
Ruoyu Wu, *Purdue University;* Taegyu Kim, *The Pennsylvania State University;* Dave (Jing) Tian, Antonio Bianchi, and Dongyan Xu, *Purdue University*

## Measurement IV

**Measurement by Proxy: On the Accuracy of Online Marketplace Measurements** . . . . . . . . . . . . . . . . . . . . . . . . . . 2153
Alejandro Cuevas, *Carnegie Mellon University;* Fieke Miedema, *Delft University of Technology;* Kyle Soska, *University of Illinois Urbana Champaign and Hikari Labs, Inc.;* Nicolas Christin, *Carnegie Mellon University and Hikari Labs, Inc.;* Rolf van Wegberg, *Delft University of Technology*

**Behind the Tube: Exploitative Monetization of Content on YouTube** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .2171
Andrew Chu, *University of Chicago;* Arjun Arunasalam, Muslum Ozgur Ozmen, and Z. Berkay Celik, *Purdue University*

**When Sally Met Trackers: Web Tracking From the Users' Perspective** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2189
Savino Dambra, *EURECOM and Norton Research Group;* Iskander Sanchez-Rola and Leyla Bilge, *Norton Research Group;* Davide Balzarotti, *EURECOM*

**How to Peel a Million: Validating and Expanding Bitcoin Clusters** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2207
George Kappos and Haaroon Yousaf, *University College London and IC3;* Rainer Stütz and Sofia Rollet, *AIT - Austrian Institute of Technology;* Bernhard Haslhofer, *Complexity Science Hub Vienna;* Sarah Meiklejohn, *University College London and IC3*

## Hardware Security II: Embedded

**RapidPatch: Firmware Hotpatching for Real-Time Embedded Devices** . . . . . . . . . . 2225
Yi He and Zhenhua Zou, *Tsinghua University and BNRist;* Kun Sun, *George Mason University;* Zhuotao Liu and Ke Xu, *Tsinghua University and BNRist;* Qian Wang, *Wuhan University;* Chao Shen, *Xi'an Jiaotong University;* Zhi Wang, *Florida State University;* Qi Li, *Tsinghua University and BNRist*

**GAROTA: Generalized Active Root-Of-Trust Architecture (for Tiny Embedded Devices)** . . . . . . . . . . 2243
Esmerald Aliaj, *University of California, Irvine;* Ivan De Oliveira Nunes, *Rochester Institute of Technology;* Gene Tsudik, *University of California, Irvine*

**ReZone: Disarming TrustZone with TEE Privilege Reduction** . . . . . . . . . . 2261
David Cerdeira and José Martins, *Centro ALGORITMI, Universidade do Minho;* Nuno Santos, *INESC-ID / Instituto Superior Técnico, Universidade de Lisboa;* Sandro Pinto, *Centro ALGORITMI, Universidade do Minho*

**Holistic Control-Flow Protection on Real-Time Embedded Systems with Kage** . . . . . . . . . . 2281
Yufei Du, *UNC Chapel Hill and University of Rochester;* Zhuojia Shen, Komail Dharsee, and Jie Zhou, *University of Rochester;* Robert J. Walls, *Worcester Polytechnic Institute;* John Criswell, *University of Rochester*

## Client-Side Security

**Orca: Blocklisting in Sender-Anonymous Messaging** . . . . . . . . . . 2299
Nirvan Tyagi and Julia Len, *Cornell University;* Ian Miers, *University of Maryland;* Thomas Ristenpart, *Cornell Tech*

**Adversarial Detection Avoidance Attacks: Evaluating the robustness of perceptual hashing-based client-side scanning** . . . . . . . . . . 2317
Shubham Jain, Ana-Maria Crețu, and Yves-Alexandre de Montjoye, *Imperial College London*

**Hecate: Abuse Reporting in Secure Messengers with Sealed Sender** . . . . . . . . . . 2335
Rawane Issa, Nicolas Alhaddad, and Mayank Varia, *Boston University*

**End-to-Same-End Encryption: Modularly Augmenting an App with an Efficient, Portable, and Blind Cloud Storage** . . . . . . . . . . 2353
Long Chen, *Institute of Software, Chinese Academy of Sciences;* Ya-Nan Li and Qiang Tang, *The University of Sydney;* Moti Yung, *Google & Columbia University*

## Crypto IV: Databases & Logging

***Omnes pro uno*: Practical Multi-Writer Encrypted Database** . . . . . . . . . . 2371
Jiafan Wang and Sherman S. M. Chow, *The Chinese University of Hong Kong*

**Faster Yet Safer: Logging System Via Fixed-Key Blockcipher** . . . . . . . . . . 2389
Viet Tung Hoang, Cong Wu, and Xin Yuan, *Florida State University*

**IHOP: Improved Statistical Query Recovery against Searchable Symmetric Encryption through Quadratic Optimization** . . . . . . . . . . 2407
Simon Oya and Florian Kerschbaum, *University of Waterloo*

**Dynamic Searchable Encryption with Optimal Search in the Presence of Deletions** . . . . . . . . . . 2425
Javad Ghareh Chamani and Dimitrios Papadopoulos, *Hong Kong University of Science and Technology;* Mohammadamin Karbasforushan and Ioannis Demertzis, *UC Santa Cruz*

## Software Forensics

**Alastor: Reconstructing the Provenance of Serverless Intrusions** . . . . . . . . . . 2443
Pubali Datta, *University of Illinois at Urbana-Champaign;* Isaac Polinsky, *North Carolina State University;* Muhammad Adil Inam and Adam Bates, *University of Illinois at Urbana-Champaign;* William Enck, *North Carolina State University*

**Back-Propagating System Dependency Impact for Attack Investigation** . . . . . . . . . . 2461
Pengcheng Fang, *Case Western Reserve University;* Peng Gao, *Virginia Tech;* Changlin Liu and Erman Ayday, *Case Western Reserve University;* Kangkook Jee, *University of Texas at Dallas;* Ting Wang, *Penn State University;* Yanfang (Fanny) Ye, *Case Western Reserve University;* Zhuotao Liu, *Tsinghua University;* Xusheng Xiao, *Case Western Reserve University*

**Ground Truth for Binary Disassembly is Not Easy** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2479
Chengbin Pang and Tiantai Zhang, *Nanjing University;* Ruotong Yu, *University of Utah;* Bing Mao, *Nanjing University;* Jun Xu, *University of Utah*

**FreeWill: Automatically Diagnosing Use-after-free Bugs via Reference Miscounting Detection on Binaries** . . . . 2497
Liang He, *TCA, Institute of Software, Chinese Academy of Sciences;* Hong Hu, *Pennsylvania State University;* Purui Su, *TCA / SKLCS, Institute of Software, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences;* Yan Cai, *SKLCS, Institute of Software, Chinese Academy of Sciences;* Zhenkai Liang, *National University of Singapore*

## Information Flow

**PolyCruise: A Cross-Language Dynamic Information Flow Analysis** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2513
Wen Li, *Washington State University, Pullman;* Jiang Ming, *University of Texas at Arlington;* Xiapu Luo, *The Hong Kong Polytechnic University;* Haipeng Cai, *Washington State University, Pullman*

**SymSan: Time and Space Efficient Concolic Execution via Dynamic Data-flow Analysis** . . . . . . . . . . . . . . . . . . . . 2531
Ju Chen, *UC Riverside;* Wookhyun Han, *KAIST;* Mingjun Yin, Haochen Zeng, and Chengyu Song, *UC Riverside;* Byoungyoung Lee, *Seoul National University;* Heng Yin, *UC Riverside;* Insik Shin, *KAIST*

**CellIFT: Leveraging Cells for Scalable and Precise Dynamic Information Flow Tracking in RTL** . . . . . . . . . . . . 2549
Flavien Solt, *ETH Zurich;* Ben Gras, *Intel Corporation;* Kaveh Razavi, *ETH Zurich*

**FlowMatrix: GPU-Assisted Information-Flow Analysis through Matrix-Based Representation** . . . . . . . . . . . . . . . . 2567
Kaihang Ji, Jun Zeng, Yuancheng Jiang, and Zhenkai Liang, *National University of Singapore;* Zheng Leong Chua, *Independent Researcher;* Prateek Saxena and Abhik Roychoudhury, *National University of Singapore*

## Network Security II: Infrastructure

**Bedrock: Programmable Network Support for Secure RDMA Systems** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2585
Jiarong Xing, Kuo-Feng Hsu, Yiming Qiu, Ziyang Yang, Hongyi Liu, and Ang Chen, *Rice University*

**Creating a Secure Underlay for the Internet** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2601
Henry Birge-Lee, *Princeton University;* Joel Wanner, *ETH Zürich;* Grace H. Cimaszewski, *Princeton University;* Jonghoon Kwon, *ETH Zürich;* Liang Wang, *Princeton University;* François Wirz, *ETH Zürich;* Prateek Mittal, *Princeton University;* Adrian Perrig, *ETH Zürich;* Yixin Sun, *University of Virginia*

**Off-Path Network Traffic Manipulation via Revitalized ICMP Redirect Attacks** . . . . . . . . . . . . . . . . . . . . . . . . . . 2619
Xuewei Feng, *Department of Computer Science and Technology & BNRist, Tsinghua University;* Qi Li, *Institute for Network Sciences and Cyberspace & BNRist, Tsinghua University and Zhongguancun Lab;* Kun Sun, *Department of Information Sciences and Technology & CSIS, George Mason University;* Zhiyun Qian, *UC Riverside;* Gang Zhao, *Department of Computer Science and Technology & BNRist, Tsinghua University;* Xiaohui Kuang, *Beijing University of Posts and Telecommunications;* Chuanpu Fu, *Department of Computer Science and Technology & BNRist, Tsinghua University;* Ke Xu, *Department of Computer Science and Technology & BNRist, Tsinghua University and Zhongguancun Lab*

***VerLoc*: Verifiable Localization in Decentralized Systems** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2637
Katharina Kohls, *Radboud University Nijmegen;* Claudia Diaz, *imec-COSIC KU Leuven and Nym Technologies SA*

## ML III

**Towards More Robust Keyword Spotting for Voice Assistants** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2655
Shimaa Ahmed, *University of Wisconsin-Madison;* Ilia Shumailov, *University of Cambridge;* Nicolas Papernot, *University of Toronto and Vector Institute;* Kassem Fawaz, *University of Wisconsin-Madison*

**Seeing is Living? Rethinking the Security of Facial Liveness Verification in the Deepfake Era** . . . . . . . . . . . . . . . . 2673
Changjiang Li, *Pennsylvania State University and Zhejiang University;* Li Wang, *Shandong University;* Shouling Ji and Xuhong Zhang, *Zhejiang University;* Zhaohan Xi, *Pennsylvania State University;* Shanqing Guo, *Shandong University;* Ting Wang, *Pennsylvania State University*

**Who Are You (I Really Wanna Know)? Detecting Audio DeepFakes Through Vocal Tract Reconstruction** . . . . . . 2691
Logan Blue, Kevin Warren, Hadi Abdullah, Cassidy Gibson, Luis Vargas, Jessica O’Dell, Kevin Butler, and Patrick Traynor, *University of Florida*

**DeepDi: Learning a Relational Graph Convolutional Network Model on Instructions for Fast and Accurate Disassembly** .......... 2709
Sheng Yu, *University of California Riverside and Deepbits Technology Inc.;* Yu Qu, *University of California Riverside;* Xunchao Hu, *Deepbits Technology Inc.;* Heng Yin, *University of California Riverside and Deepbits Technology Inc.*

## Security Practitioners & Behaviors

**RE-Mind: a First Look Inside the Mind of a Reverse Engineer** .......... 2727
Alessandro Mantovani and Simone Aonzo, *EURECOM;* Yanick Fratantonio, *Cisco Talos;* Davide Balzarotti, *EURECOM*

**Characterizing the Security of Github CI Workflows** ...........2747
Igibek Koishybayev and Aleksandr Nahapetyan, *North Carolina State University;* Raima Zachariah, *Independent Researcher;* Siddharth Muralee, *Purdue University;* Bradley Reaves and Alexandros Kapravelos, *North Carolina State University;* Aravind Machiry, *Purdue University*

**Decomperson: How Humans Decompile and What We Can Learn From It** .......... 2765
Kevin Burk, Fabio Pagani, Christopher Kruegel, and Giovanni Vigna, *UC Santa Barbara*

**99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms** .......... 2783
Bushra A. Alahmadi, Louise Axon, and Ivan Martinovic, *University of Oxford*

## Side Channels II

**HyperDegrade: From GHz to MHz Effective CPU Frequencies** .......... 2801
Alejandro Cabrera Aldaya and Billy Bob Brumley, *Tampere University*

**Pacer: Comprehensive Network Side-Channel Mitigation in the Cloud** .......... 2819
Aastha Mehta, *University of British Columbia* (*UBC*)*;* Mohamed Alzayat, Roberta De Viti, Björn B. Brandenburg, Peter Druschel, and Deepak Garg, *Max Planck Institute for Software Systems* (*MPI-SWS*)

**Composable Cachelets: Protecting Enclaves from Cache Side-Channel Attacks** .......... 2839
Daniel Townley, *Peraton Labs;* Kerem Arıkan, Yu David Liu, and Dmitry Ponomarev, *Binghamton University;* Oğuz Ergin, *TOBB University of Economics and Technology*

**Don't Mesh Around: Side-Channel Attacks and Mitigations on Mesh Interconnects** .......... 2857
Miles Dai, *MIT;* Riccardo Paccagnella, *University of Illinois at Urbana-Champaign;* Miguel Gomez-Garcia, *MIT;* John McCalpin, *Texas Advanced Computing Center;* Mengjia Yan, *MIT*

## Web Security V: Tracking

**WebGraph: Capturing Advertising and Tracking Information Flows for Robust Blocking** .......... 2875
Sandra Siby, *EPFL;* Umar Iqbal, *University of Iowa;* Steven Englehardt, *DuckDuckGo;* Zubair Shafiq, *UC Davis;* Carmela Troncoso, *EPFL*

**Automating Cookie Consent and GDPR Violation Detection** .......... 2893
Dino Bollinger, Karel Kubicek, Carlos Cotrini, and David Basin, *ETH Zurich*

**Khaleesi: Breaker of Advertising and Tracking Request Chains** .......... 2911
Umar Iqbal, *University of Washington;* Charlie Wolfe, *University of Iowa;* Charles Nguyen, *University of California, Davis;* Steven Englehardt, *DuckDuckGo;* Zubair Shafiq, *University of California, Davis*

**Practical Data Access Minimization in Trigger-Action Platforms** .......... 2929
Yunang Chen and Mohannad Alhanahnah, *University of Wisconsin–Madison;* Andrei Sabelfeld, *Chalmers University of Technology;* Rahul Chatterjee and Earlence Fernandes, *University of Wisconsin–Madison*

## Crypto V: Provers & Shuffling

**Shuffle-based Private Set Union: Faster and More Secure** .......... 2947
Yanxue Jia and Shi-Feng Sun, *Shanghai Jiao Tong University;* Hong-Sheng Zhou, *Virginia Commonwealth University;* Jiajun Du and Dawu Gu, *Shanghai Jiao Tong University*

**Polynomial Commitment with a One-to-Many Prover and Applications** .......... 2965
Jiaheng Zhang and Tiancheng Xie, *UC Berkeley;* Thang Hoang, *Virginia Tech;* Elaine Shi, *CMU;* Yupeng Zhang, *Texas A&M University*

**ppSAT: Towards Two-Party Private SAT Solving** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2983
Ning Luo, Samuel Judson, Timos Antonopoulos, and Ruzica Piskac, *Yale University;* Xiao Wang, *Northwestern University*

**Hyperproofs: Aggregating and Maintaining Proofs in Vector Commitments** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3001
Shravan Srinivasan, *University of Maryland;* Alexander Chepurnoy, *Ergo Platform;* Charalampos Papamanthou, *Yale University;* Alin Tomescu, *VMware Research;* Yupeng Zhang, *Texas A&M University*

## Friday, August 12

### Security Analysis

**COMRace: Detecting Data Race Vulnerabilities in COM Objects** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3019
Fangming Gu and Qingli Guo, *Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences;* Lian Li, *Institute of Computing Technology, Chinese Academy of Sciences and School of Computer Science and Technology, University of Chinese Academy of Sciences;* Zhiniang Peng, *Sangfor Technologies Inc and Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences;* Wei Lin, Xiaobo Yang, and Xiaorui Gong, *Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences*

**Movery: A Precise Approach for Modified Vulnerable Code Clone Discovery from Modified Open-Source Software Components** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3037
Seunghoon Woo, Hyunji Hong, Eunjin Choi, and Heejo Lee, *Korea University*

**Loki: Hardening Code Obfuscation Against Automated Attacks** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3055
Moritz Schloegel, Tim Blazytko, Moritz Contag, Cornelius Aschermann, and Julius Basler, *Ruhr-Universität Bochum;* Thorsten Holz, *CISPA Helmholtz Center for Information Security;* Ali Abbasi, *Ruhr-Universität Bochum*

**Oops... Code Execution and Content Spoofing: The First Comprehensive Analysis of OpenDocument Signatures** . . 3075
Simon Rohlmann, Christian Mainka, Vladislav Mladenov, and Jörg Schwenk, *Ruhr University Bochum*

**Playing Without Paying: Detecting Vulnerable Payment Verification in Native Binaries of Unity Mobile Games** . . 3093
Chaoshun Zuo and Zhiqiang Lin, *The Ohio State University*

### SGX I & Side Channels III

**Repurposing Segmentation as a Practical LVI-NULL Mitigation in SGX** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .3111
Lukas Giner, Andreas Kogler, and Claudio Canella, *Graz University of Technology;* Michael Schwarz, *CISPA Helmholtz Center for Information Security;* Daniel Gruss, *Graz University of Technology*

**A Hardware-Software Co-design for Efficient Intra-Enclave Isolation** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3129
Jinyu Gu, Bojun Zhu, Mingyu Li, Wentai Li, Yubin Xia, and Haibo Chen, *Shanghai Jiao Tong University*

**SGXFuzz: Efficiently Synthesizing Nested Structures for SGX Enclave Fuzzing** . . . . . . . . . . . . . . . . . . . . . . . . . . . .3147
Tobias Cloosters, *University of Duisburg-Essen;* Johannes Willbold, *Ruhr-Universität Bochum;* Thorsten Holz, *CISPA Helmholtz Center for Information Security;* Lucas Davi, *University of Duisburg-Essen*

**SecSMT: Securing SMT Processors against Contention-Based Covert Channels** . . . . . . . . . . . . . . . . . . . . . . . . . . . .3165
Mohammadkazem Taram, *University of California San Diego;* Xida Ren and Ashish Venkat, *University of Virginia;* Dean Tullsen, *University of California San Diego*

**Rendering Contention Channel Made Practical in Web Browsers** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3183
Shujiang Wu and Jianjia Yu, *Johns Hopkins University;* Min Yang, *Fudan University;* Yinzhi Cao, *Johns Hopkins University*

### Fuzzing III

**SyzScope: Revealing High-Risk Security Impacts of Fuzzer-Exposed Bugs in Linux kernel** . . . . . . . . . . . . . . . . . . 3201
Xiaochen Zou, Guoren Li, Weiteng Chen, Hang Zhang, and Zhiyun Qian, *UC Riverside*

***TheHuzz*: Instruction Fuzzing of Processors Using Golden-Reference Models for Finding Software-Exploitable Vulnerabilities** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3219
Rahul Kande, Addison Crump, and Garrett Persyn, *Texas A&M University;* Patrick Jauernig and Ahmad-Reza Sadeghi, *Technische Universität Darmstadt;* Aakash Tyagi and Jeyavijayan Rajendran, *Texas A&M University*

**Fuzzing Hardware Like Software** . . . . . . . . . . 3237
Timothy Trippel and Kang G. Shin, *University of Michigan;* Alex Chernyakhovsky, Garret Kelly, and Dominic Rizzo, *Google, LLC;* Matthew Hicks, *Virginia Tech*

**Stateful Greybox Fuzzing** . . . . . . . . . . 3255
Jinsheng Ba, *National University of Singapore;* Marcel Böhme, *Monash University and MPI-SP;* Zahra Mirzamomen, *Monash University;* Abhik Roychoudhury, *National University of Singapore*

**StateFuzz: System Call-Based State-Aware Linux Driver Fuzzing** . . . . . . . . . . 3273
Bodong Zhao, Zheming Li, Shisong Qin, Zheyu Ma, and Ming Yuan, *Institute for Network Science and Cyberspace / BNRist, Tsinghua University;* Wenyu Zhu, *Department of Electronic Engineering, Tsinghua University;* Zhihong Tian, *Guangzhou University;* Chao Zhang, *Institute for Network Science and Cyberspace / BNRist, Tsinghua University and Zhongguancun Lab*

## Crypto VI

**How to Abuse and Fix Authenticated Encryption Without Key Commitment** . . . . . . . . . . 3291
Ange Albertini and Thai Duong, *Google Research;* Shay Gueron, *University of Haifa and Amazon;* Stefan Kölbl, Atul Luykx, and Sophie Schmieg, *Google Research*

**Private Signaling** . . . . . . . . . . 3309
Varun Madathil and Alessandra Scafuro, *North Carolina State University;* István András Seres, *Eötvös Loránd University;* Omer Shlomovits and Denis Varlakov, *ZenGo X*

**Batched Differentially Private Information Retrieval** . . . . . . . . . . 3327
Kinan Dak Albab, *Brown University;* Rawane Issa and Mayank Varia, *Boston University;* Kalman Graffi, *Honda Research Institute Europe*

**Practical Privacy-Preserving Authentication for SSH** . . . . . . . . . . 3345
Lawrence Roy, Stanislav Lyakhov, Yeongjin Jang, and Mike Rosulek, *Oregon State University*

**One-off Disclosure Control by Heterogeneous Generalization** . . . . . . . . . . 3363
Olga Gkountouna, *University of Liverpool;* Katerina Doka, *National Technical University of Athens;* Mingqiang Xue, *Tower Research;* Jianneng Cao, *Bank Jago;* Panagiotis Karras, *Aarhus University*

## User Studies III: Privacy

**Understanding and Improving Usability of Data Dashboards for Simplified Privacy Control of Voice Assistant Data** . . . . . . . . . . 3379
Vandit Sharma and Mainack Mondal, *Indian Institute of Technology Kharagpur*

**Security and Privacy Perceptions of Third-Party Application Access for Google Accounts** . . . . . . . . . . 3397
David G. Balash, Xiaoyuan Wu, and Miles Grant, *The George Washington University;* Irwin Reyes, *Two Six Technologies;* Adam J. Aviv, *The George Washington University*

**Empirical Understanding of Deletion Privacy: Experiences, Expectations, and Measures** . . . . . . . . . . 3415
Mohsen Minaei, *Purdue University;* Mainack Mondal, *IIT Kharagpur;* Aniket Kate, *Purdue University*

**Security at the End of the Tunnel: The Anatomy of VPN Mental Models Among Experts and Non-Experts in a Corporate Context** . . . . . . . . . . 3433
Veroniek Binkhorst, *Technical University of Delft;* Tobias Fiebig, *Max-Planck-Institut für Informatik and Technical University of Delft;* Katharina Krombholz, *CISPA Helmholtz Center for Information Security;* Wolter Pieters, *Radboud University;* Katsiaryna Labunets, *Utrecht University*

**How and Why People Use Virtual Private Networks** . . . . . . . . . . 3451
Agnieszka Dutkowska-Zuk, *Lancaster University;* Austin Hounsel, *Princeton University;* Amy Morrill, *University of Chicago;* Andre Xiong, *Princeton University;* Marshini Chetty and Nick Feamster, *University of Chicago*

## Smart Homes II

**CamShield: Securing Smart Cameras through Physical Replication and Isolation** . . . . . . . . . . 3467
Zhiwei Wang, Yihui Yan, and Yueli Yan, *ShanghaiTech University;* Huangxun Chen, *Huawei Theory Lab;* Zhice Yang, *ShanghaiTech University*

**SCRAPS: Scalable Collective Remote Attestation for Pub-Sub IoT Networks with Untrusted Proxy Verifier . . . . 3485**
Lukas Petzi, Ala Eddine Ben Yahya, and Alexandra Dmitrienko, *University of Würzburg;* Gene Tsudik, *UC Irvine;* Thomas Prantl and Samuel Kounev, *University of Würzburg*

**An Experimental Study of GPS Spoofing and Takeover Attacks on UAVs . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3503**
Harshad Sathaye, *Northeastern University;* Martin Strohmeier and Vincent Lenders, *armasuisse;* Aanjhan Ranganathan, *Northeastern University*

**Smart Home Privacy Policies Demystified: A Study of Availability, Content, and Coverage . . . . . . . . . . . . . . . . . . . 3521**
Sunil Manandhar and Kaushal Kafle, *William & Mary;* Benjamin Andow, *Google LLC;* Kapil Singh, *IBM T.J. Watson Research Center;* Adwait Nadkarni, *William & Mary*

**MaDIoT 2.0: Modern High-Wattage IoT Botnet Attacks and Defenses . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3539**
Tohid Shekari, *Georgia Institute of Technology;* Alvaro A. Cardenas, *University of California, Santa Cruz;* Raheem Beyah, *Georgia Institute of Technology*

## ML IV: Attacks

**AutoDA: Automated Decision-based Iterative Adversarial Attacks . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3557**
Qi-An Fu, *Dept. of Comp. Sci. and Tech., Institute for AI, Tsinghua-Bosch Joint ML Center, THBI Lab, BNRist Center, Tsinghua University, Beijing, China;* Yinpeng Dong, *Dept. of Comp. Sci. and Tech., Institute for AI, Tsinghua-Bosch Joint ML Center, THBI Lab, BNRist Center, Tsinghua University, Beijing, China; RealAI;* Hang Su, *Dept. of Comp. Sci. and Tech., Institute for AI, Tsinghua-Bosch Joint ML Center, THBI Lab, BNRist Center, Tsinghua University, Beijing, China; Peng Cheng Laboratory; Tsinghua University-China Mobile Communications Group Co., Ltd. Joint Institute;* Jun Zhu, *Dept. of Comp. Sci. and Tech., Institute for AI, Tsinghua-Bosch Joint ML Center, THBI Lab, BNRist Center, Tsinghua University, Beijing, China; RealAI; Peng Cheng Laboratory; Tsinghua University-China Mobile Communications Group Co., Ltd. Joint Institute;* Chao Zhang, *Institute for Network Science and Cyberspace / BNRist, Tsinghua University*

**Poison Forensics: Traceback of Data Poisoning Attacks in Neural Networks . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3575**
Shawn Shan, Arjun Nitin Bhagoji, Haitao Zheng, and Ben Y. Zhao, *University of Chicago*

**Teacher Model Fingerprinting Attacks Against Transfer Learning . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3593**
Yufei Chen, *Xi'an Jiaotong University & City University of Hong Kong;* Chao Shen, *Xi'an Jiaotong University;* Cong Wang, *City University of Hong Kong;* Yang Zhang, *CISPA Helmholtz Center for Information Security*

**Hidden Trigger Backdoor Attack on NLP Models via Linguistic Style Manipulation . . . . . . . . . . . . . . . . . . . . . . . . .3611**
Xudong Pan, Mi Zhang, Beina Sheng, Jiaming Zhu, and Min Yang, *Fudan University*

**PoisonedEncoder: Poisoning the Unlabeled Pre-training Data in Contrastive Learning . . . . . . . . . . . . . . . . . . . . . . 3629**
Hongbin Liu, Jinyuan Jia, and Neil Zhenqiang Gong, *Duke University*

## Fuzzing, OS, and Cloud Security

**Double Trouble: Combined Heterogeneous Attacks on Non-Inclusive Cache Hierarchies . . . . . . . . . . . . . . . . . . . . . 3647**
Antoon Purnal, Furkan Turan, and Ingrid Verbauwhede, *imec-COSIC, KU Leuven*

**QuORAM: A Quorum-Replicated Fault Tolerant ORAM Datastore . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3665**
Sujaya Maiyya, Seif Ibrahim, Caitlin Scarberry, Divyakant Agrawal, and Amr El Abbadi, *UC Santa Barbara;* Huijia Lin and Stefano Tessaro, *University of Washington;* Victor Zakhary, *Oracle*

**Post-Quantum Cryptography with Contemporary Co-Processors: Beyond Kronecker, Schönhage-Strassen & Nussbaumer . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3683**
Joppe W. Bos, Joost Renes, and Christine van Vredendaal, *NXP Semiconductors*

**FixReverter: A Realistic Bug Injection Methodology for Benchmarking Fuzz Testing . . . . . . . . . . . . . . . . . . . . . . 3699**
Zenong Zhang and Zach Patterson, *University of Texas at Dallas;* Michael Hicks, *University of Maryland and Amazon;* Shiyi Wei, *University of Texas at Dallas*

**Tightly Seal Your Sensitive Pointers with PACTight . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .3717**
Mohannad Ismail, *Virginia Tech;* Andrew Quach, *Oregon State University;* Christopher Jelesnianski, *Virginia Tech;* Yeongjin Jang, *Oregon State University;* Changwoo Min, *Virginia Tech*

## Privacy, User Behaviors, and Attacks

**Total Eclipse of the Heart – Disrupting the InterPlanetary File System** .......... **3735**
Bernd Prünster, *Institute of Applied Information Processing and Communications (IAIK), Graz University of Technology;* Alexander Marsalek, *A-SIT Secure Information Technology Center Austria;* Thomas Zefferer, *A-SIT Plus GmbH*

**PrivGuard: Privacy Regulation Compliance Made Easier** .......... **3753**
Lun Wang, *UC Berkeley;* Usmann Khan, *Georgia Tech;* Joseph Near, *University of Vermont;* Qi Pang, *Zhejiang University;* Jithendaraa Subramanian, *NIT Tiruchirappalli;* Neel Somani, *UC Berkeley;* Peng Gao, *Virginia Tech;* Andrew Low and Dawn Song, *UC Berkeley*

**Stick It to The Man: Correcting for Non-Cooperative Behavior of Subjects in Experiments on Social Networks** . **3771**
Kaleigh Clary, *University of Massachusetts Amherst;* Emma Tosch and Jeremiah Onaolapo, *University of Vermont;* David D. Jensen, *University of Massachusetts Amherst*

**OVRseen: Auditing Network Traffic and Privacy Policies in Oculus VR** .......... **3789**
Rahmadi Trimananda, Hieu Le, Hao Cui, and Janice Tran Ho, *University of California, Irvine;* Anastasia Shuba, *Independent Researcher;* Athina Markopoulou, *University of California, Irvine*

## Hardware Security III

**Half-Double: Hammering From the Next Row Over** .......... **3807**
Andreas Kogler, *Graz University of Technology;* Jonas Juffinger, *Graz University of Technology and Lamarr Security Research;* Salman Qazi and Yoongu Kim, *Google;* Moritz Lipp, *Amazon Web Services;* Nicolas Boichat, *Google;* Eric Shiu, *Rivos;* Mattias Nissler, *Google;* Daniel Gruss, *Graz University of Technology*

**Retbleed: Arbitrary Speculative Code Execution with Return Instructions** .......... **3825**
Johannes Wikner and Kaveh Razavi, *ETH Zurich*

**PISTIS: Trusted Computing Architecture for Low-end Embedded Systems** .......... **3843**
Michele Grisafi, *University of Trento;* Mahmoud Ammar, *Huawei Technologies;* Marco Roveri and Bruno Crispo, *University of Trento*

**Rapid Prototyping for Microarchitectural Attacks** .......... **3861**
Catherine Easdon, *Dynatrace Research and Graz University of Technology;* Michael Schwarz, *CISPA Helmholtz Center for Information Security;* Martin Schwarzl and Daniel Gruss, *Graz University of Technology*

## OS Security & Formalisms

**ProFactory: Improving IoT Security via Formalized Protocol Customization** .......... **3879**
Fei Wang, Jianliang Wu, and Yuhong Nan, *Purdue University;* Yousra Aafer, *University of Waterloo;* Xiangyu Zhang and Dongyan Xu, *Purdue University;* Mathias Payer, *EPFL*

**Using Trāṭṛ to tame Adversarial Synchronization** .......... **3897**
Yuvraj Patel, Chenhao Ye, Akshat Sinha, Abigail Matthews, Andrea C. Arpaci-Dusseau, Remzi H. Arpaci-Dusseau, and Michael M. Swift, *University of Wisconsin–Madison*

**ÆPIC Leak: Architecturally Leaking Uninitialized Data from the Microarchitecture** ..........**3917**
Pietro Borrello, *Sapienza University of Rome;* Andreas Kogler and Martin Schwarzl, *Graz University of Technology;* Moritz Lipp, *Amazon Web Services;* Daniel Gruss, *Graz University of Technology;* Michael Schwarz, *CISPA Helmholtz Center for Information Security*

**Sapic$^+$: protocol verifiers of the world, unite!** .......... **3935**
Vincent Cheval, *Inria Paris;* Charlie Jacomme, *CISPA Helmholtz Center for Information Security;* Steve Kremer, *Université de Lorraine LORIA & Inria Nancy;* Robert Künnemann, *CISPA Helmholtz Center for Information Security*

## ML V: Principles & Best Practices

**On the Security Risks of AutoML** .......... **3953**
Ren Pang and Zhaohan Xi, *Pennsylvania State University;* Shouling Ji, *Zhejiang University;* Xiapu Luo, *Hong Kong Polytechnic University;* Ting Wang, *Pennsylvania State University*

**Dos and Don'ts of Machine Learning in Computer Security** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **3971**
Daniel Arp, *Technische Universität Berlin;* Erwin Quiring, *Technische Universität Braunschweig;* Feargus Pendlebury, *King's College London and Royal Holloway, University of London and The Alan Turing Institute;* Alexander Warnecke, *Technische Universität Braunschweig;* Fabio Pierazzi, *King's College London;* Christian Wressnegger, *KASTEL Security Research Labs and Karlsruhe Institute of Technology;* Lorenzo Cavallaro, *University College London;* Konrad Rieck, *Technische Universität Braunschweig*

**Exploring the Security Boundary of Data Reconstruction via Neuron Exclusivity Analysis** . . . . . . . . . . . . . . . . . . **3989**
Xudong Pan, Mi Zhang, Yifan Yan, Jiaming Zhu, and Min Yang, *Fudan University*

**On the Necessity of Auditable Algorithmic Definitions for Machine Unlearning** . . . . . . . . . . . . . . . . . . . . . . . . . . **4007**
Anvith Thudi, Hengrui Jia, Ilia Shumailov, and Nicolas Papernot, *University of Toronto & Vector Institute*

## User Studies IV: Policies & Best Practices

**"The Same PIN, Just Longer": On the (In)Security of Upgrading PINs from 4 to 6 Digits** . . . . . . . . . . . . . . . . . . . . **4023**
Collins W. Munyendo, *The George Washington University;* Philipp Markert, *Ruhr University Bochum;* Alexandra Nisenoff, *University of Chicago;* Miles Grant and Elena Korkes, *The George Washington University;* Blase Ur, *University of Chicago;* Adam J. Aviv, *The George Washington University*

**Where to Recruit for Security Development Studies: Comparing Six Software Developer Samples** . . . . . . . . . . . . . **4041**
Harjot Kaur, *Leibniz University Hannover;* Sabrina Amft, *CISPA Helmholtz Center for Information Security;* Daniel Votipka, *Tufts University;* Yasemin Acar, *Max Planck Institute for Security and Privacy and George Washington University;* Sascha Fahl, *CISPA Helmholtz Center for Information Security and Leibniz University Hannover*

**Investigating State-of-the-Art Practices for Fostering Subjective Trust in Online Voting through Interviews** . . . . **4059**
Karola Marky, *Leibniz University Hannover and University of Glasgow;* Paul Gerber and Sebastian Günther, *Technical University of Darmstadt;* Mohamed Khamis, *University of Glasgow;* Maximilian Fries and Max Mühlhäuser, *Technical University of Darmstadt*

**Electronic Monitoring Smartphone Apps: An Analysis of Risks from Technical, Human-Centered, and Legal Perspectives** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **4077**
Kentrell Owens, *University of Washington;* Anita Alem, *Harvard Law School;* Franziska Roesner and Tadayoshi Kohno, *University of Washington*

## SGX II

**Mage: Mutual Attestation for a Group of Enclaves without Trusted Third Parties** . . . . . . . . . . . . . . . . . . . . . . . . . **4095**
Guoxing Chen, *Shanghai Jiao Tong University;* Yinqian Zhang, *Southern University of Science and Technology*

**Elasticlave: An Efficient Memory Model for Enclaves** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **.4111**
Jason Zhijingcheng Yu, *National University of Singapore;* Shweta Shinde, *ETH Zurich;* Trevor E. Carlson and Prateek Saxena, *National University of Singapore*

**SGXLock: Towards Efficiently Establishing Mutual Distrust Between Host Application and Enclave for SGX** . . **4129**
Yuan Chen, Jiaqi Li, Guorui Xu, and Yajin Zhou, *Zhejiang University;* Zhi Wang, *Florida State University;* Cong Wang, *City University of Hong Kong;* Kui Ren, *Zhejiang University*

**Minefield: A Software-only Protection for SGX Enclaves against DVFS Attacks** . . . . . . . . . . . . . . . . . . . . . . . . . . . **.4147**
Andreas Kogler and Daniel Gruss, *Graz University of Technology;* Michael Schwarz, *CISPA Helmholtz Center for Information Security*

## Network Security III: DDoS

**Counting in Regexes Considered Harmful: Exposing ReDoS Vulnerability of Nonbacktracking Matchers** . . . . . . **.4165**
Lenka Turoňová, Lukáš Holík, Ivan Homoliak, and Ondřej Lengál, *Faculty of Information Technology, Brno University of Technology;* Margus Veanes, *Microsoft Research Redmond;* Tomáš Vojnar, *Faculty of Information Technology, Brno University of Technology*

**RegexScalpel: Regular Expression Denial of Service (ReDoS) Defense by Localize-and-Fix . . . . . . . . . . . . . . . . . . 4183**
Yeting Li, *CAS-KLONAT, Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences; SKLCS, Institute of Software, Chinese Academy of Sciences;* Yecheng Sun, *SKLCS, Institute of Software, Chinese Academy of Sciences; University of Chinese Academy of Sciences;* Zhiwu Xu, *College of Computer Science and Software Engineering, Shenzhen University;* Jialun Cao, *The Hong Kong University of Science and Technology;* Yuekang Li, *School of Computer Science and Engineering, Nanyang Technological University;* Rongchen Li, *SKLCS, Institute of Software, Chinese Academy of Sciences; University of Chinese Academy of Sciences;* Haiming Chen, *SKLCS, Institute of Software, Chinese Academy of Sciences; CAS-KLONAT, Institute of Information Engineering, Chinese Academy of Sciences;* Shing-Chi Cheung, *The Hong Kong University of Science and Technology;* Yang Liu, *School of Computer Science and Engineering, Nanyang Technological University;* Yang Xiao, *CAS-KLONAT, Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences*

**Anycast Agility: Network Playbooks to Fight DDoS . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4201**
A S M Rizvi, *USC/ISI;* Leandro Bertholdo, *University of Twente;* João Ceron, *SIDN Labs;* John Heidemann, *USC/ISI*

**Regulator: Dynamic Analysis to Detect ReDoS . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4219**
Robert McLaughlin, Fabio Pagani, Noah Spahn, Christopher Kruegel, and Giovanni Vigna, *University of California, Santa Barbara*

## Zero Knowledge

**Aardvark: An Asynchronous Authenticated Dictionary with Applications to Account-based Cryptocurrencies . . 4237**
Derek Leung, *MIT CSAIL;* Yossi Gilad, *Hebrew University of Jerusalem;* Sergey Gorbunov, *University of Waterloo;* Leonid Reyzin, *Boston University;* Nickolai Zeldovich, *MIT CSAIL*

**Zero-Knowledge Middleboxes . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4255**
Paul Grubbs, Arasu Arun, Ye Zhang, Joseph Bonneau, and Michael Walfish, *NYU*

**Efficient Representation of Numerical Optimization Problems for SNARKs . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4273**
Sebastian Angel, *University of Pennsylvania and Microsoft Research;* Andrew J. Blumberg, *Columbia University;* Eleftherios Ioannidis and Jess Woods, *University of Pennsylvania*

**Experimenting with Collaborative zk-SNARKs: Zero-Knowledge Proofs for Distributed Secrets . . . . . . . . . . . . . . 4291**
Alex Ozdemir and Dan Boneh, *Stanford University*

## Software Security

**Detecting Logical Bugs of DBMS with Coverage-based Guidance . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4309**
Yu Liang, *Pennsylvania State University;* Song Liu, *Pennsylvania State University and Qi-AnXin Tech. Research Institute;* Hong Hu, *Pennsylvania State University*

**Augmenting Decompiler Output with Learned Variable Names and Types . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4327**
Qibin Chen and Jeremy Lacomis, *Carnegie Mellon University;* Edward J. Schwartz, *Carnegie Mellon University Software Engineering Institute;* Claire Le Goues, Graham Neubig, and Bogdan Vasilescu, *Carnegie Mellon University*

**Debloating Address Sanitizer . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4345**
Yuchen Zhang, *Stevens Institute of Technology;* Chengbin Pang, *Nanjing University;* Georgios Portokalidis, Nikos Triandopoulos, and Jun Xu, *Stevens Institute of Technology*

**Ferry: State-Aware Symbolic Execution for Exploring State-Dependent Program Paths . . . . . . . . . . . . . . . . . . . . . 4365**
Shunfan Zhou, Zhemin Yang, and Dan Qiao, *Fudan University;* Peng Liu, *The Pennsylvania State University;* Min Yang, *Fudan University;* Zhe Wang and Chenggang Wu, *State Key Laboratory of Computer Architecture, Institute of Computing Technology, Chinese Academy of Sciences*

## Side Channels IV

**Can one hear the shape of a neural network?: Snooping the GPU via Magnetic Side Channel . . . . . . . . . . . . . . . . . 4383**
Henrique Teles Maia and Chang Xiao, *Columbia University;* Dingzeyu Li, *Adobe Research;* Eitan Grinspun, *Columbia University & University of Toronto;* Changxi Zheng, *Columbia University*

**Lamphone: Passive Sound Recovery from a Desk Lamp's Light Bulb Vibrations . . . . . . . . . . . . . . . . . . . . . . . . . . . 4401**
Ben Nassi, Yaron Pirutin, and Raz Swisa, *Ben-Gurion University of the Negev;* Adi Shamir, *Weizmann Institute of Science;* Yuval Elovici and Boris Zadov, *Ben-Gurion University of the Negev*

**Automated Side Channel Analysis of Media Software with Manifold Learning** . . . . . . . . . . . . . . . . . . . . . . . . . . . . **4419**
Yuanyuan Yuan, Qi Pang, and Shuai Wang, *The Hong Kong University of Science and Technology*

**Lend Me Your Ear: Passive Remote Physical Side Channels on PCs** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **4437**
Daniel Genkin, *Georgia Tech;* Noam Nissan, *Tel Aviv University;* Roei Schuster, *Tel Aviv University and Cornell Tech;* Eran Tromer, *Tel Aviv University and Columbia University*

## Network Security IV

**Stalloris: RPKI Downgrade Attack** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **4455**
Tomas Hlavacek and Philipp Jeitner, *Fraunhofer Institute for Secure Information Technology SIT and National Research Center for Applied Cybersecurity ATHENE;* Donika Mirdita, *Fraunhofer Institute for Secure Information Technology SIT, National Research Center for Applied Cybersecurity ATHENE, and Technische Universität Darmstadt;* Haya Shulman, *Fraunhofer Institute for Secure Information Technology SIT, National Research Center for Applied Cybersecurity ATHENE, and Goethe-Universität Frankfurt;* Michael Waidner, *Fraunhofer Institute for Secure Information Technology SIT, National Research Center for Applied Cybersecurity ATHENE, and Technische Universität Darmstadt*

**XDRI Attacks - and - How to Enhance Resilience of Residential Routers** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **4473**
Philipp Jeitner, *Fraunhofer Institute for Secure Information Technology SIT and National Research Center for Applied Cybersecurity ATHENE;* Haya Shulman, *Fraunhofer Institute for Secure Information Technology SIT, National Research Center for Applied Cybersecurity ATHENE, and Goethe-Universität Frankfurt;* Lucas Teichmann, *Fraunhofer Institute for Secure Information Technology SIT;* Michael Waidner, *Fraunhofer Institute for Secure Information Technology SIT, National Research Center for Applied Cybersecurity ATHENE, and Technische Universität Darmstadt*

**V'CER: Efficient Certificate Validation in Constrained Networks** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **4491**
David Koisser and Patrick Jauernig, *Technical University Darmstadt;* Gene Tsudik, *University of California, Irvine;* Ahmad-Reza Sadeghi, *Technical University Darmstadt*

**Themis: Accelerating the Detection of Route Origin Hijacking by Distinguishing Legitimate and Illegitimate MOAS** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **4509**
Lancheng Qin, *Tsinghua University;* Dan Li, *Tsinghua University and Zhongguancun Laboratory;* Ruifeng Li, *Tsinghua Shenzhen International Graduate School;* Kang Wang, *Tsinghua University*

## ML VI: Inference

**ML-Doctor: Holistic Risk Assessment of Inference Attacks Against Machine Learning Models** . . . . . . . . . . . . . . **4525**
Yugeng Liu, Rui Wen, Xinlei He, Ahmed Salem, Zhikun Zhang, and Michael Backes, *CISPA Helmholtz Center for Information Security;* Emiliano De Cristofaro, *UCL and Alan Turing Institute;* Mario Fritz and Yang Zhang, *CISPA Helmholtz Center for Information Security*

**Inference Attacks Against Graph Neural Networks** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **4543**
Zhikun Zhang, Min Chen, and Michael Backes, *CISPA Helmholtz Center for Information Security;* Yun Shen, *Norton Research Group;* Yang Zhang, *CISPA Helmholtz Center for Information Security*

**Membership Inference Attacks and Defenses in Neural Network Pruning** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **4561**
Xiaoyong Yuan and Lan Zhang, *Michigan Technological Unviersity*

**Are Your Sensitive Attributes Private? Novel Model Inversion Attribute Inference Attacks on Classification Models** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . **4579**
Shagufta Mehnaz, *The Pennsylvania State University;* Sayanton V. Dibbo and Ehsanul Kabir, *Dartmouth College;* Ninghui Li and Elisa Bertino, *Purdue University*