

# 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 Uncharted 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 Doupe, 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*

**Midass: 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*

<b>FUGIO: Automatic Exploit Generation for PHP Object Injection Vulnerabilities</b> .....	197
Sunnyeo Park and Daejun Kim, <i>KAIST</i> ; Suman Jana, <i>Columbia University</i> ; Soeul Son, <i>KAIST</i>	
<b>Crypto I: Attacking Implementations</b>	
<b>TLS-Anvil: Adapting Combinatorial Testing for TLS Libraries</b> .....	215
Marcel Maehren and Philipp Nieting, <i>Ruhr University Bochum</i> ; Sven Hebrok, <i>Paderborn University</i> ; Robert Merget, <i>Ruhr University Bochum</i> ; Juraj Somorovsky, <i>Paderborn University</i> ; Jörg Schwenk, <i>Ruhr University Bochum</i>	
<b>Open to a fault: On the passive compromise of TLS keys via transient errors</b> .....	233
George Arnold Sullivan, <i>University of California, San Diego</i> ; Jackson Sippe, <i>University of Colorado Boulder</i> ; Nadia Heninger, <i>University of California, San Diego</i> ; Eric Wustrow, <i>University of Colorado Boulder</i>	
<b>Trust Dies in Darkness: Shedding Light on Samsung's TrustZone Keymaster Design</b> .....	251
Alon Shakevsky, Eyal Ronen, and Avishai Wool, <i>Tel-Aviv University</i>	
<b>Breaking Bridgefy, again: Adopting libsignal is not enough</b> .....	269
Martin R. Albrecht, <i>Information Security Group, Royal Holloway, University of London</i> ; Raphael Eikenberg and Kenneth G. Paterson, <i>Applied Cryptography Group, ETH Zurich</i>	
<b>User Studies I: At-Risk Users</b>	
<b>"I feel invaded, annoyed, anxious and I may protect myself": Individuals' Feelings about Online Tracking and their Protective Behaviour across Gender and Country</b> .....	287
Kovila P.L. Coopamootoo and Maryam Mehrnezhad, <i>Newcastle University</i> ; Ehsan Toreini, <i>Durham University</i>	
<b>"Like Lesbians Walking the Perimeter": Experiences of U.S. LGBTQ+ Folks With Online Security, Safety, and Privacy Advice</b> .....	305
Christine Geeng and Mike Harris, <i>University of Washington</i> ; Elissa Redmiles, <i>Max Planck Institute for Software Systems</i> ; Franziska Roesner, <i>University of Washington</i>	
<b>"They Look at Vulnerability and Use That to Abuse You": Participatory Threat Modelling with Migrant Domestic Workers</b> .....	323
Julia Słupska and Selina Cho, <i>University of Oxford</i> ; Marissa Begonia, <i>Voice of Domestic Workers</i> ; Ruba Abu-Salma, <i>King's College London</i> ; Nayanatara Prakash, <i>University of Oxford</i> ; Mallika Balakrishnan, <i>Migrants Organise</i>	
<b>Networks of Care: Tech Abuse Advocates' Digital Security Practices</b> .....	341
Julia Slupska, <i>University of Oxford</i> ; Angelika Strohmayer, <i>Northumbria University</i>	
<b>Software Vulnerabilities</b>	
<b>How Long Do Vulnerabilities Live in the Code? A Large-Scale Empirical Measurement Study on FOSS Vulnerability Lifetimes</b> .....	359
Nikolaos Alexopoulos, Manuel Brack, Jan Philipp Wagner, Tim Grube, and Max Mühlhäuser, <i>Technical University of Darmstadt</i>	
<b>Expected Exploitability: Predicting the Development of Functional Vulnerability Exploits</b> .....	377
Octavian Suciu, <i>University of Maryland, College Park</i> ; Connor Nelson, Zhuoer Lyu, and Tiffany Bao, <i>Arizona State University</i> ; Tudor Dumitraş, <i>University of Maryland, College Park</i>	
<b>OS-Aware Vulnerability Prioritization via Differential Severity Analysis</b> .....	395
Qiusi Wu, <i>University of Minnesota</i> ; Yue Xiao and Xiaojing Liao, <i>Indiana University Bloomington</i> ; Kangjie Lu, <i>University of Minnesota</i>	
<b>Arbiter: Bridging the Static and Dynamic Divide in Vulnerability Discovery on Binary Programs</b> .....	413
Jayakrishna Vadayath, <i>Arizona State University</i> ; Moritz Eckert, <i>EURECOM</i> ; Kyle Zeng, <i>Arizona State University</i> ; Nicolaas Weideman, <i>University of Southern California</i> ; Gokulkrishna Praveen Menon, <i>Arizona State University</i> ; Yanick Fratantonio, <i>Cisco Systems Inc.</i> ; Davide Balzarotti, <i>EURECOM</i> ; Adam Doupé, Tiffany Bao, and Ruoyu Wang, <i>Arizona State University</i> ; Christophe Hauser, <i>University of Southern California</i> ; Yan Shoshitaishvili, <i>Arizona State University</i>	

## Network Security I: Scanning & Censorship

<b>Spoki: Unveiling a New Wave of Scanners through a Reactive Network Telescope</b> .....	431
Raphael Hiesgen, <i>HAW Hamburg</i> ; Marcin Nawrocki, <i>Freie Universität Berlin</i> ; Alistair King, <i>Kentik</i> ; Alberto Dainotti, <i>CAIDA, UC San Diego and Georgia Institute of Technology</i> ; Thomas C. Schmidt, <i>HAW Hamburg</i> ; Matthias Wählisch, <i>Freie Universität Berlin</i>	
<b>Many Roads Lead To Rome: How Packet Headers Influence DNS Censorship Measurement</b> .....	449
Abhishek Bhaskar and Paul Pearce, <i>Georgia Institute of Technology</i>	
<b>GET /out: Automated Discovery of Application-Layer Censorship Evasion Strategies</b> .....	465
Michael Harry, Kevin Bock, Frederick Sell, and Dave Levin, <i>University of Maryland</i>	
<b>OpenVPN is Open to VPN Fingerprinting</b> .....	483
Diwen Xue, Reethika Ramesh, and Arham Jain, <i>University of Michigan</i> ; Michalis Kallitsis, <i>Merit Network, Inc.</i> ; J. Alex Halderman, <i>University of Michigan</i> ; Jedidiah R. Crandall, <i>Arizona State University/Breakpointing Bad</i> ; Roya Ensafi, <i>University of Michigan</i>	

## Differential Privacy

<b>Pool Inference Attacks on Local Differential Privacy: Quantifying the Privacy Guarantees of Apple's Count Mean Sketch in Practice</b> .....	501
Andrea Gadotti, <i>Imperial College London</i> ; Florimond Houssiau, <i>Alan Turing Institute</i> ; Meenatchi Sundaram Muthu Selva Annamalai and Yves-Alexandre de Montjoye, <i>Imperial College London</i>	
<b>Poisoning Attacks to Local Differential Privacy Protocols for Key-Value Data</b> .....	519
Yongji Wu, Xiaoyu Cao, Jinyuan Jia, and Neil Zhenqiang Gong, <i>Duke University</i>	
<b>Communication-Efficient Triangle Counting under Local Differential Privacy</b> .....	537
Jacob Imola, <i>UC San Diego</i> ; Takao Murakami, <i>AIST</i> ; Kamalika Chaudhuri, <i>UC San Diego</i>	
<b>Twilight: A Differentially Private Payment Channel Network</b> .....	555
Maya Dotan, Saar Tochner, Aviv Zohar, and Yossi Gilad, <i>The Hebrew University of Jerusalem</i>	

## Measurement II: Auditing & Best Practices

<b>Watching the watchers: bias and vulnerability in remote proctoring software</b> .....	571
Ben Burgess, <i>Princeton University</i> ; Avi Ginsberg, <i>Georgetown Law</i> ; Edward W. Felten, <i>Princeton University</i> ; Shaanan Cohney, <i>University of Melbourne</i>	
<b>The Antrim County 2020 Election Incident: An Independent Forensic Investigation</b> .....	589
J. Alex Halderman, <i>University of Michigan</i>	
<b>An Audit of Facebook's Political Ad Policy Enforcement</b> .....	607
Victor Le Pochat, <i>imec-DistriNet, KU Leuven</i> ; Laura Edelson, <i>New York University</i> ; Tom Van Goethem and Wouter Joosen, <i>imec-DistriNet, KU Leuven</i> ; Damon McCoy and Tobias Lauinger, <i>New York University</i>	
<b>Building an Open, Robust, and Stable Voting-Based Domain Top List</b> .....	625
Qinge Xie, <i>Georgia Institute of Technology</i> ; Shujun Tang, <i>QI-ANXIN Technology Research Institute</i> ; Xiaofeng Zheng, <i>QI-ANXIN Technology Research Institute and Tsinghua University</i> ; Qingran Lin, <i>QI-ANXIN Technology Research Institute</i> ; Baojun Liu, <i>Tsinghua University</i> ; Haixin Duan, <i>QI-ANXIN Technology Research Institute and Tsinghua University</i> ; Frank Li, <i>Georgia Institute of Technology</i>	

## Side Channels I: Hardware

<b>AMD Prefetch Attacks through Power and Time</b> .....	643
Moritz Lipp and Daniel Gruss, <i>Graz University of Technology</i> ; Michael Schwarz, <i>CISPA Helmholtz Center for Information Security</i>	
<b>Hiding in Plain Sight? On the Efficacy of Power Side Channel-Based Control Flow Monitoring</b> .....	661
Yi Han, Matthew Chan, and Zahra Aref, <i>Rutgers University</i> ; Nils Ole Tippenhauer, <i>CISPA Helmholtz Center for Information Security</i> ; Saman Zonouz, <i>Georgia Tech</i>	

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

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

## Web Security II: Fingerprinting

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

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

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

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

## Crypto II: Performance Improvements

<b>Secure Poisson Regression</b> . . . . .	791
Mahimna Kelkar, <i>Cornell Tech</i> ; Phi Hung Le, Mariana Raykova, and Karn Seth, <i>Google</i>	

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

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

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

## User Studies II: Sharing

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

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

<b>Caring about Sharing: User Perceptions of Multiparty Data Sharing</b> . . . . .	899
Bailey Kacsmar, Kyle Tilbury, Miti Mazmudar, and Florian Kerschbaum, <i>University of Waterloo</i>	

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

## Hardware Security I: Attacks & Defenses

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

**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*; Wenyan 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*



<b>A Large-scale Investigation into Geodifferences in Mobile Apps</b> .....	1203
Renuka Kumar, Apurva Virkud, Ram Sundara Raman, Atul Prakash, and Roya Ensafi, <i>University of Michigan</i>	
<b>Fuzzing II: Low-Level</b>	
<b>MORPHUZZ: Bending (Input) Space to Fuzz Virtual Devices</b> .....	1221
Alexander Bulekov, <i>Boston University and Red Hat</i> ; Bandan Das and Stefan Hajnoczi, <i>Red Hat</i> ; Manuel Egele, <i>Boston University</i>	
<b>Fuzzware: Using Precise MMIO Modeling for Effective Firmware Fuzzing</b> .....	1239
Tobias Scharnowski, Nils Bars, and Moritz Schloegel, <i>Ruhr-Universität Bochum</i> ; Eric Gustafson, <i>UC Santa Barbara</i> ; Marius Muench, <i>Vrije Universiteit Amsterdam</i> ; Giovanni Vigna, <i>UC Santa Barbara and VMware</i> ; Christopher Kruegel, <i>UC Santa Barbara</i> ; Thorsten Holz and Ali Abbasi, <i>Ruhr-Universität Bochum</i>	
<b>MUNDOFUZZ: Hypervisor Fuzzing with Statistical Coverage Testing and Grammar Inference</b> .....	1257
Cheolwoo Myung, Gwangmu Lee, and Byoungyoung Lee, <i>Seoul National University</i>	
<b>Drifuzz: Harvesting Bugs in Device Drivers from Golden Seeds</b> .....	1275
Zekun Shen, Ritik Roongta, and Brendan Dolan-Gavitt, <i>NYU</i>	
<b>Wireless Security</b>	
<b>LTRACK: Stealthy Tracking of Mobile Phones in LTE</b> .....	1291
Martin Kotuliak, Simon Erni, Patrick Leu, Marc Röschlin, and Srdjan Čapkun, <i>ETH Zurich</i>	
<b>Watching the Watchers: Practical Video Identification Attack in LTE Networks</b> .....	1307
Sangwook Bae, Mincheol Son, Dongkwan Kim, CheolJun Park, Jiho Lee, Sooel Son, and Yongdae Kim, <i>Korea Advanced Institute of Science and Technology (KAIST)</i>	
<b>DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices</b> .....	1325
CheolJun Park, Sangwook Bae, BeomSeok Oh, Jiho Lee, Eunkyu Lee, Insu Yun, and Yongdae Kim, <i>Korea Advanced Institute of Science and Technology (KAIST)</i>	
<b>Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging</b> .....	1343
Patrick Leu and Giovanni Camurati, <i>ETH Zurich</i> ; Alexander Heinrich, <i>TU Darmstadt</i> ; Marc Roeschlin and Claudio Anliker, <i>ETH Zurich</i> ; Matthias Hollick, <i>TU Darmstadt</i> ; Srdjan Capkun, <i>ETH Zurich</i> ; Jiska Classen, <i>TU Darmstadt</i>	
<b>ML I: Federated Learning</b>	
<b>SIMC: ML Inference Secure Against Malicious Clients at Semi-Honest Cost</b> .....	1361
Nishanth Chandran, Divya Gupta, and Sai Lakshmi Bhavana Obbattu, <i>Microsoft Research</i> ; Akash Shah, <i>UCLA</i>	
<b>Efficient Differentially Private Secure Aggregation for Federated Learning via Hardness of Learning with Errors</b> .....	1379
Timothy Stevens, Christian Skalka, and Christelle Vincent, <i>University of Vermont</i> ; John Ring, <i>MassMutual</i> ; Samuel Clark, <i>Raytheon</i> ; Joseph Near, <i>University of Vermont</i>	
<b>Label Inference Attacks Against Vertical Federated Learning</b> .....	1397
Chong Fu, <i>Zhejiang University</i> ; Xuhong Zhang and Shouling Ji, <i>Binjiang Institute of Zhejiang University</i> ; Jinyin Chen, <i>Zhejiang University of Technology</i> ; Jingzheng Wu, <i>Institute of Software, Chinese Academy of Sciences</i> ; Shanqing Guo, <i>Shandong University</i> ; Jun Zhou and Alex X. Liu, <i>Ant Group</i> ; Ting Wang, <i>Pennsylvania State University</i>	
<b>FLAME: Taming Backdoors in Federated Learning</b> .....	1415
Thien Duc Nguyen and Phillip Rieger, <i>Technical University of Darmstadt</i> ; Huili Chen, <i>University of California San Diego</i> ; Hossein Yalame, Helen Möllering, and Hossein Fereidooni, <i>Technical University of Darmstadt</i> ; Samuel Marchal, <i>Aalto University and F-Secure</i> ; Markus Miettinen, <i>Technical University of Darmstadt</i> ; Azalia Mirhoseini, <i>Google</i> ; Shaza Zeitouni, <i>Technical University of Darmstadt</i> ; Farinaz Koushanfar, <i>University of California San Diego</i> ; Ahmad-Reza Sadeghi and Thomas Schneider, <i>Technical University of Darmstadt</i>	

## 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 Ceconello, 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*

<b>Constant-weight PIR: Single-round Keyword PIR via Constant-weight Equality Operators .....</b>	<b>1723</b>
Rasoul Akhavan Mahdavi and Florian Kerschbaum, <i>University of Waterloo</i>	
<b>Incremental Offline/Online PIR .....</b>	<b>1741</b>
Yiping Ma and Ke Zhong, <i>University of Pennsylvania</i> ; Tal Rabin, <i>University of Pennsylvania and Algorand Foundation</i> ; Sebastian Angel, <i>University of Pennsylvania and Microsoft Research</i>	
<b>GPU-accelerated PIR with Client-Independent Preprocessing for Large-Scale Applications .....</b>	<b>1759</b>
Daniel Günther and Maurice Heymann, <i>Technical University of Darmstadt</i> ; Benny Pinkas, <i>Bar-Ilan University</i> ; Thomas Schneider, <i>Technical University of Darmstadt</i>	
<b>Increasing Adversarial Uncertainty to Scale Private Similarity Testing .....</b>	<b>1777</b>
Yiqing Hua and Armin Namavari, <i>Cornell Tech and Cornell University</i> ; Kaishuo Cheng, <i>Cornell University</i> ; Mor Naaman and Thomas Ristenpart, <i>Cornell Tech and Cornell University</i>	
<b>Passwords</b>	
<b>Pre-hijacked accounts: An Empirical Study of Security Failures in User Account Creation on the Web. ....</b>	<b>1795</b>
Avinash Sudhodanan, <i>Independent Researcher</i> ; Andrew Paverd, <i>Microsoft Security Response Center</i>	
<b>Leaky Forms: A Study of Email and Password Exfiltration Before Form Submission. ....</b>	<b>1813</b>
Asuman Senol, <i>imec-COSIC, KU Leuven</i> ; Gunes Acar, <i>Radboud University</i> ; Mathias Humbert, <i>University of Lausanne</i> ; Frederik Zuiderveen Borgesius, <i>Radboud University</i>	
<b>Might I Get Pwned: A Second Generation Compromised Credential Checking Service .....</b>	<b>1831</b>
Bijeta Pal, <i>Cornell University</i> ; Mazharul Islam, <i>University of Wisconsin–Madison</i> ; Marina Sanusi Bohuk, <i>Cornell University</i> ; Nick Sullivan, Luke Valenta, Tara Whalen, and Christopher Wood, <i>Cloudflare</i> ; Thomas Ristenpart, <i>Cornell Tech</i> ; Rahul Chatterjee, <i>University of Wisconsin–Madison</i>	
<b>Why Users (Don’t) Use Password Managers at a Large Educational Institution .....</b>	<b>1849</b>
Peter Mayer, <i>Karlsruhe Institute of Technology</i> ; Collins W. Munyendo, <i>The George Washington University</i> ; Michelle L. Mazurek, <i>University of Maryland, College Park</i> ; Adam J. Aviv, <i>The George Washington University</i>	
<b>Gossamer: Securely Measuring Password-based Logins .....</b>	<b>1867</b>
Marina Sanusi Bohuk, <i>Cornell University</i> ; Mazharul Islam, <i>University of Wisconsin–Madison</i> ; Suleman Ahmad, <i>Cloudflare</i> ; Michael Swift, <i>University of Wisconsin–Madison</i> ; Thomas Ristenpart, <i>Cornell Tech</i> ; Rahul Chatterjee, <i>University of Wisconsin–Madison</i>	
<b>Smart Vehicles</b>	
<b>DoubleStar: Long-Range Attack Towards Depth Estimation based Obstacle Avoidance in Autonomous Systems. ....</b>	<b>1885</b>
Ce Zhou, Qiben Yan, and Yan Shi, <i>Michigan State University</i> ; Lichao Sun, <i>Lehigh University</i>	
<b>Security Analysis of Camera-LiDAR Fusion Against Black-Box Attacks on Autonomous Vehicles .....</b>	<b>1903</b>
R. Spencer Hallyburton and Yupei Liu, <i>Duke University</i> ; Yulong Cao and Z. Morley Mao, <i>University of Michigan</i> ; Miroslav Pajic, <i>Duke University</i>	
<b>SAID: State-aware Defense Against Injection Attacks on In-vehicle Network .....</b>	<b>1921</b>
Lei Xue, <i>The Hong Kong Polytechnic University Shenzhen Research Institute</i> ; Yangyang Liu, Tianqi Li, Kaifa Zhao, Jianfeng Li, Le Yu, and Xiapu Luo, <i>The Hong Kong Polytechnic University</i> ; Yajin Zhou, <i>Zhejiang University</i> ; Guofei Gu, <i>Texas A&amp;M University</i>	
<b>Towards Automatically Reverse Engineering Vehicle Diagnostic Protocols .....</b>	<b>1939</b>
Le Yu, Yangyang Liu, Pengfei Jing, Xiapu Luo, Lei Xue, and Kaifa Zhao, <i>The Hong Kong Polytechnic University</i> ; Yajin Zhou, <i>Zhejiang University</i> ; Ting Wang, <i>The Pennsylvania State University</i> ; Guofei Gu, <i>Texas A&amp;M University</i> ; Sen Nie and Shi Wu, <i>Tencent Keen Security Lab</i>	
<b>Rolling Colors: Adversarial Laser Exploits against Traffic Light Recognition .....</b>	<b>1957</b>
Chen Yan, <i>Zhejiang University</i> ; Zhijian Xu, <i>Zhejiang University and The Chinese University of Hong Kong</i> ; Zhanyuan Yin, <i>The University of Chicago</i> ; Xiaoyu Ji and Wenyan Xu, <i>Zhejiang University</i>	



## 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 Earlene 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 Haaron 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*

**SYM<sub>SAN</sub>: 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*

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

## Security Practitioners & Behaviors

<b>RE-Mind: a First Look Inside the Mind of a Reverse Engineer</b> .....	<b>2727</b>
Alessandro Mantovani and Simone Aonzo, <i>EURECOM</i> ; Yanick Fratantonio, <i>Cisco Talos</i> ; Davide Balzarotti, <i>EURECOM</i>	
<b>Characterizing the Security of Github CI Workflows</b> .....	<b>2747</b>
Igibek Koishybayev and Aleksandr Nahapetyan, <i>North Carolina State University</i> ; Raima Zachariah, <i>Independent Researcher</i> ; Siddharth Muralee, <i>Purdue University</i> ; Bradley Reaves and Alexandros Kapravelos, <i>North Carolina State University</i> ; Aravind Machiry, <i>Purdue University</i>	
<b>DECOMPERSON: How Humans Decompile and What We Can Learn From It</b> .....	<b>2765</b>
Kevin Burk, Fabio Pagani, Christopher Kruegel, and Giovanni Vigna, <i>UC Santa Barbara</i>	
<b>99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms</b> .....	<b>2783</b>
Bushra A. Alahmadi, Louise Axon, and Ivan Martinovic, <i>University of Oxford</i>	

## Side Channels II

<b>HyperDegrade: From GHz to MHz Effective CPU Frequencies</b> .....	<b>2801</b>
Alejandro Cabrera Aldaya and Billy Bob Brumley, <i>Tampere University</i>	
<b>Pacer: Comprehensive Network Side-Channel Mitigation in the Cloud</b> .....	<b>2819</b>
Aastha Mehta, <i>University of British Columbia (UBC)</i> ; Mohamed Alzayat, Roberta De Viti, Björn B. Brandenburg, Peter Druschel, and Deepak Garg, <i>Max Planck Institute for Software Systems (MPI-SWS)</i>	
<b>Composable Cachelets: Protecting Enclaves from Cache Side-Channel Attacks</b> .....	<b>2839</b>
Daniel Townley, <i>Peraton Labs</i> ; Kerem Arıkan, Yu David Liu, and Dmitry Ponomarev, <i>Binghamton University</i> ; Oğuz Ergin, <i>TOBB University of Economics and Technology</i>	
<b>Don't Mesh Around: Side-Channel Attacks and Mitigations on Mesh Interconnects</b> .....	<b>2857</b>
Miles Dai, <i>MIT</i> ; Riccardo Paccagnella, <i>University of Illinois at Urbana-Champaign</i> ; Miguel Gomez-Garcia, <i>MIT</i> ; John McCalpin, <i>Texas Advanced Computing Center</i> ; Mengjia Yan, <i>MIT</i>	

## Web Security V: Tracking

<b>WEBGRAPH: Capturing Advertising and Tracking Information Flows for Robust Blocking</b> .....	<b>2875</b>
Sandra Siby, <i>EPFL</i> ; Umar Iqbal, <i>University of Iowa</i> ; Steven Englehardt, <i>DuckDuckGo</i> ; Zubair Shafiq, <i>UC Davis</i> ; Carmela Troncoso, <i>EPFL</i>	
<b>Automating Cookie Consent and GDPR Violation Detection</b> .....	<b>2893</b>
Dino Bollinger, Karel Kubicek, Carlos Cotrini, and David Basin, <i>ETH Zurich</i>	
<b>KHALEESI: Breaker of Advertising and Tracking Request Chains</b> .....	<b>2911</b>
Umar Iqbal, <i>University of Washington</i> ; Charlie Wolfe, <i>University of Iowa</i> ; Charles Nguyen, <i>University of California, Davis</i> ; Steven Englehardt, <i>DuckDuckGo</i> ; Zubair Shafiq, <i>University of California, Davis</i>	
<b>Practical Data Access Minimization in Trigger-Action Platforms</b> .....	<b>2929</b>
Yunang Chen and Mohannad Alhanahnah, <i>University of Wisconsin–Madison</i> ; Andrei Sabelfeld, <i>Chalmers University of Technology</i> ; Rahul Chatterjee and Earlene Fernandes, <i>University of Wisconsin–Madison</i>	

## Crypto V: Provers & Shuffling

<b>Shuffle-based Private Set Union: Faster and More Secure</b> .....	<b>2947</b>
Yanxue Jia and Shi-Feng Sun, <i>Shanghai Jiao Tong University</i> ; Hong-Sheng Zhou, <i>Virginia Commonwealth University</i> ; Jiajun Du and Dawu Gu, <i>Shanghai Jiao Tong University</i>	
<b>Polynomial Commitment with a One-to-Many Prover and Applications</b> .....	<b>2965</b>
Jiaheng Zhang and Tiancheng Xie, <i>UC Berkeley</i> ; Thang Hoang, <i>Virginia Tech</i> ; Elaine Shi, <i>CMU</i> ; Yupeng Zhang, <i>Texas A&amp;M University</i>	



<b>ppSAT: Towards Two-Party Private SAT Solving</b> .....	<b>2983</b>
Ning Luo, Samuel Judson, Timos Antonopoulos, and Ruzica Piskac, <i>Yale University</i> ; Xiao Wang, <i>Northwestern University</i>	
<b>Hyperproofs: Aggregating and Maintaining Proofs in Vector Commitments</b> .....	<b>3001</b>
Shravan Srinivasan, <i>University of Maryland</i> ; Alexander Chepur, <i>Ergo Platform</i> ; Charalampos Papamanthou, <i>Yale University</i> ; Alin Tomescu, <i>VMware Research</i> ; Yupeng Zhang, <i>Texas A&amp;M University</i>	

## Friday, August 12

### Security Analysis

<b>COMRACE: Detecting Data Race Vulnerabilities in COM Objects</b> .....	<b>3019</b>
Fangming Gu and Qingli Guo, <i>Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences</i> ; Lian Li, <i>Institute of Computing Technology, Chinese Academy of Sciences and School of Computer Science and Technology, University of Chinese Academy of Sciences</i> ; Zhiniang Peng, <i>Sangfor Technologies Inc and Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences</i> ; Wei Lin, Xiaobo Yang, and Xiaorui Gong, <i>Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences</i>	
<b>MOVERY: A Precise Approach for Modified Vulnerable Code Clone Discovery from Modified Open-Source Software Components</b> .....	<b>3037</b>
Seunghoon Woo, Hyunji Hong, Eunjin Choi, and Heejo Lee, <i>Korea University</i>	
<b>Loki: Hardening Code Obfuscation Against Automated Attacks</b> .....	<b>3055</b>
Moritz Schloegel, Tim Blazytko, Moritz Contag, Cornelius Aschermann, and Julius Basler, <i>Ruhr-Universität Bochum</i> ; Thorsten Holz, <i>CISPA Helmholtz Center for Information Security</i> ; Ali Abbasi, <i>Ruhr-Universität Bochum</i>	
<b>Oops... Code Execution and Content Spoofing: The First Comprehensive Analysis of OpenDocument Signatures</b> ..	<b>3075</b>
Simon Rohlmann, Christian Mainka, Vladislav Mladenov, and Jörg Schwenk, <i>Ruhr University Bochum</i>	
<b>Playing Without Paying: Detecting Vulnerable Payment Verification in Native Binaries of Unity Mobile Games</b> ..	<b>3093</b>
Chaoshun Zuo and Zhiqiang Lin, <i>The Ohio State University</i>	

### SGX I & Side Channels III

<b>Repurposing Segmentation as a Practical LVI-NULl Mitigation in SGX</b> .....	<b>3111</b>
Lukas Giner, Andreas Kogler, and Claudio Canella, <i>Graz University of Technology</i> ; Michael Schwarz, <i>CISPA Helmholtz Center for Information Security</i> ; Daniel Gruss, <i>Graz University of Technology</i>	
<b>A Hardware-Software Co-design for Efficient Intra-Enclave Isolation</b> .....	<b>3129</b>
Jinyu Gu, Bojun Zhu, Mingyu Li, Wentai Li, Yubin Xia, and Haibo Chen, <i>Shanghai Jiao Tong University</i>	
<b>SGXFuzz: Efficiently Synthesizing Nested Structures for SGX Enclave Fuzzing</b> .....	<b>3147</b>
Tobias Cloosters, <i>University of Duisburg-Essen</i> ; Johannes Willbold, <i>Ruhr-Universität Bochum</i> ; Thorsten Holz, <i>CISPA Helmholtz Center for Information Security</i> ; Lucas Davi, <i>University of Duisburg-Essen</i>	
<b>SecSMT: Securing SMT Processors against Contention-Based Covert Channels</b> .....	<b>3165</b>
Mohammadkazem Taram, <i>University of California San Diego</i> ; Xida Ren and Ashish Venkat, <i>University of Virginia</i> ; Dean Tullsen, <i>University of California San Diego</i>	
<b>Rendering Contention Channel Made Practical in Web Browsers</b> .....	<b>3183</b>
Shujiang Wu and Jianjia Yu, <i>Johns Hopkins University</i> ; Min Yang, <i>Fudan University</i> ; Yinzhao Cao, <i>Johns Hopkins University</i>	

### Fuzzing III

<b>SyzScope: Revealing High-Risk Security Impacts of Fuzzer-Exposed Bugs in Linux kernel</b> .....	<b>3201</b>
Xiaochen Zou, Guoren Li, Weiteng Chen, Hang Zhang, and Zhiyun Qian, <i>UC Riverside</i>	
<b>TheHuzz: Instruction Fuzzing of Processors Using Golden-Reference Models for Finding Software-Exploitable Vulnerabilities</b> .....	<b>3219</b>
Rahul Kande, Addison Crump, and Garrett Persyn, <i>Texas A&amp;M University</i> ; Patrick Jauernig and Ahmad-Reza Sadeghi, <i>Technische Universität Darmstadt</i> ; Aakash Tyagi and Jeyavijayan Rajendran, <i>Texas A&amp;M University</i>	



**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 Albal, *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*; Usman 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 Trätr 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, Iliia 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 Klivan, *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*



<b>RegexScalpel: Regular Expression Denial of Service (ReDoS) Defense by Localize-and-Fix .....</b>	<b>4183</b>
Yeting Li, CAS-KLONAT, <i>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</i>	
<b>Anycast Agility: Network Playbooks to Fight DDoS.....</b>	<b>4201</b>
A S M Rizvi, USC/ISI; Leandro Bertholdo, <i>University of Twente</i> ; João Ceron, <i>SIDN Labs</i> ; John Heidemann, <i>USC/ISI</i>	
<b>Regulator: Dynamic Analysis to Detect ReDoS.....</b>	<b>4219</b>
Robert McLaughlin, Fabio Pagani, Noah Spahn, Christopher Kruegel, and Giovanni Vigna, <i>University of California, Santa Barbara</i>	
<b>Zero Knowledge</b>	
<b>Aardvark: An Asynchronous Authenticated Dictionary with Applications to Account-based Cryptocurrencies ..</b>	<b>4237</b>
Derek Leung, <i>MIT CSAIL</i> ; Yossi Gilad, <i>Hebrew University of Jerusalem</i> ; Sergey Gorbunov, <i>University of Waterloo</i> ; Leonid Reyzin, <i>Boston University</i> ; Nickolai Zeldovich, <i>MIT CSAIL</i>	
<b>Zero-Knowledge Middleboxes .....</b>	<b>4255</b>
Paul Grubbs, Arasu Arun, Ye Zhang, Joseph Bonneau, and Michael Walfish, <i>NYU</i>	
<b>Efficient Representation of Numerical Optimization Problems for SNARKs .....</b>	<b>4273</b>
Sebastian Angel, <i>University of Pennsylvania and Microsoft Research</i> ; Andrew J. Blumberg, <i>Columbia University</i> ; Eleftherios Ioannidis and Jess Woods, <i>University of Pennsylvania</i>	
<b>Experimenting with Collaborative zk-SNARKs: Zero-Knowledge Proofs for Distributed Secrets.....</b>	<b>4291</b>
Alex Ozdemir and Dan Boneh, <i>Stanford University</i>	
<b>Software Security</b>	
<b>Detecting Logical Bugs of DBMS with Coverage-based Guidance .....</b>	<b>4309</b>
Yu Liang, <i>Pennsylvania State University</i> ; Song Liu, <i>Pennsylvania State University and Qi-AnXin Tech. Research Institute</i> ; Hong Hu, <i>Pennsylvania State University</i>	
<b>Augmenting Decompiler Output with Learned Variable Names and Types .....</b>	<b>4327</b>
Qibin Chen and Jeremy Lacomis, <i>Carnegie Mellon University</i> ; Edward J. Schwartz, <i>Carnegie Mellon University Software Engineering Institute</i> ; Claire Le Goues, Graham Neubig, and Bogdan Vasilescu, <i>Carnegie Mellon University</i>	
<b>Debloating Address Sanitizer .....</b>	<b>4345</b>
Yuchen Zhang, <i>Stevens Institute of Technology</i> ; Chengbin Pang, <i>Nanjing University</i> ; Georgios Portokalidis, Nikos Triandopoulos, and Jun Xu, <i>Stevens Institute of Technology</i>	
<b>Ferry: State-Aware Symbolic Execution for Exploring State-Dependent Program Paths .....</b>	<b>4365</b>
Shunfan Zhou, Zhemin Yang, and Dan Qiao, <i>Fudan University</i> ; Peng Liu, <i>The Pennsylvania State University</i> ; Min Yang, <i>Fudan University</i> ; Zhe Wang and Chenggang Wu, <i>State Key Laboratory of Computer Architecture, Institute of Computing Technology, Chinese Academy of Sciences</i>	
<b>Side Channels IV</b>	
<b>Can one hear the shape of a neural network?: Snooping the GPU via Magnetic Side Channel.....</b>	<b>4383</b>
Henrique Teles Maia and Chang Xiao, <i>Columbia University</i> ; Dingzeyu Li, <i>Adobe Research</i> ; Eitan Grinspun, <i>Columbia University &amp; University of Toronto</i> ; Changxi Zheng, <i>Columbia University</i>	
<b>Lamphone: Passive Sound Recovery from a Desk Lamp’s Light Bulb Vibrations .....</b>	<b>4401</b>
Ben Nassi, Yaron Pirutin, and Raz Swisa, <i>Ben-Gurion University of the Negev</i> ; Adi Shamir, <i>Weizmann Institute of Science</i> ; Yuval Elovici and Boris Zadov, <i>Ben-Gurion University of the Negev</i>	



**Automated Side Channel Analysis of Media Software with Manifold Learning** ..... 4419  
Yuan 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 University*

**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*