

# 32nd USENIX Security Symposium

August 9–11, 2023

Anaheim, CA, USA

## Wednesday, August 9

### Breaking Wireless Protocols

**PhyAuth: Physical-Layer Message Authentication for ZigBee Networks** . . . . . 1  
Ang Li and Jiawei Li, *Arizona State University*; Dianqi Han, *University of Texas at Arlington*; Yan Zhang, *The University of Akron*; Tao Li, *Indiana University–Purdue University Indianapolis*; Ting Zhu, *The Ohio State University*;  
Yanchao Zhang, *Arizona State University*

**Time for Change: How Clocks Break UWB Secure Ranging** . . . . . 19  
Claudio Anliker, Giovanni Camurati, and Srdjan Čapkun, *ETH Zurich*

**Formal Analysis and Patching of BLE-SC Pairing** . . . . . 37  
Min Shi, Jing Chen, Kun He, Haoran Zhao, Meng Jia, and Ruiying Du, *Wuhan University*

**Framing Frames: Bypassing Wi-Fi Encryption by Manipulating Transmit Queues** . . . . . 53  
Domien Schepers and Aanjhan Ranganathan, *Northeastern University*; Mathy Vanhoef, *imec-DistriNet, KU Leuven*

### Interpersonal Abuse

**Abuse Vectors: A Framework for Conceptualizing IoT-Enabled Interpersonal Abuse** . . . . . 69  
Sophie Stephenson and Majed Almansoori, *University of Wisconsin–Madison*; Pardis Emami-Naeini, *Duke University*;  
Danny Yuxing Huang, *New York University*; Rahul Chatterjee, *University of Wisconsin–Madison*

**The Digital-Safety Risks of Financial Technologies for Survivors of Intimate Partner Violence** . . . . . 87  
Rosanna Bellini, *Cornell University*; Kevin Lee, *Princeton University*; Megan A. Brown, *Center for Social Media and Politics, New York University*; Jeremy Shaffer, *Cornell University*; Rasika Bhalerao, *Northeastern University*;  
Thomas Ristenpart, *Cornell Tech*

**“It’s the Equivalent of Feeling Like You’re in Jail”: Lessons from Firsthand and Secondhand Accounts of IoT-Enabled Intimate Partner Abuse** . . . . . 105  
Sophie Stephenson and Majed Almansoori, *University of Wisconsin–Madison*; Pardis Emami-Naeini, *Duke University*;  
Rahul Chatterjee, *University of Wisconsin–Madison*

**Sneaky Spy Devices and Defective Detectors: The Ecosystem of Intimate Partner Surveillance with Covert Devices** . . . . . 123  
Rose Ceccio and Sophie Stephenson, *University of Wisconsin–Madison*; Varun Chadha, *Capital One*;  
Danny Yuxing Huang, *New York University*; Rahul Chatterjee, *University of Wisconsin–Madison*

### Inferring User Details

**Towards a General Video-based Keystroke Inference Attack** . . . . . 141  
Zhuolin Yang, Yuxin Chen, and Zain Sarwar, *University of Chicago*; Hadleigh Schwartz, *Columbia University*;  
Ben Y. Zhao and Haitao Zheng, *University of Chicago*

**Going through the motions: AR/VR keylogging from user head motions** . . . . . 159  
Carter Slocum, Yicheng Zhang, Nael Abu-Ghazaleh, and Jiasi Chen, *University of California, Riverside*

**Auditory Eyesight: Demystifying  $\mu$ s-Precision Keystroke Tracking Attacks on Unconstrained Keyboard Inputs** . . . 175  
Yazhou Tu, Liqun Shan, and Md Imran Hossen, *University of Louisiana at Lafayette*; Sara Rampazzi and Kevin Butler, *University of Florida*; Xiali Hei, *University of Louisiana at Lafayette*

**Watch your Watch: Inferring Personality Traits from Wearable Activity Trackers** . . . . . 193  
Noé Zufferey and Mathias Humbert, *University of Lausanne, Switzerland*; Romain Tavenard, *University of Rennes, CNRS, LETG, France*; Kévin Huguenin, *University of Lausanne, Switzerland*

## Adversarial ML beyond ML

### **Squint Hard Enough: Attacking Perceptual Hashing with Adversarial Machine Learning . . . . . 211**

Jonathan Prokos, *Johns Hopkins University*; Neil Fendley, *Johns Hopkins University Applied Physics Laboratory*; Matthew Green, *Johns Hopkins University*; Roei Schuster, *Vector Institute*; Eran Tromer, *Tel Aviv University and Columbia University*; Tushar Jois and Yinzhi Cao, *Johns Hopkins University*

### **How to Cover up Anomalous Accesses to Electronic Health Records . . . . . 229**

Xiaojun Xu, Qingying Hao, Zhuolin Yang, and Bo Li, *University of Illinois at Urbana-Champaign*; David Liebovitz, *Northwestern University*; Gang Wang and Carl A. Gunter, *University of Illinois at Urbana-Champaign*

### **KENKU: Towards Efficient and Stealthy Black-box Adversarial Attacks against ASR Systems . . . . . 247**

Xinghui Wu, *Xi'an Jiaotong University*; Shiqing Ma, *University of Massachusetts Amherst*; Chao Shen and Chenhao Lin, *Xi'an Jiaotong University*; Qian Wang, *Wuhan University*; Qi Li, *Tsinghua University*; Yuan Rao, *Xi'an Jiaotong University*

### **Tubes Among Us: Analog Attack on Automatic Speaker Identification . . . . . 265**

Shimaa Ahmed and Yash Wani, *University of Wisconsin-Madison*; Ali Shahin Shamsabadi, *Alan Turing Institute*; Mohammad Yaghini, *University of Toronto and Vector Institute*; Ilia Shumailov, *Vector Institute and University of Oxford*; Nicolas Papernot, *University of Toronto and Vector Institute*; Kassem Fawaz, *University of Wisconsin-Madison*

## Private Set Operations

### **Efficient Unbalanced Private Set Intersection Cardinality and User-friendly Privacy-preserving Contact Tracing . . 283**

Mingli Wu and Tsz Hon Yuen, *The University of Hong Kong*

### **Near-Optimal Oblivious Key-Value Stores for Efficient PSI, PSU and Volume-Hiding Multi-Maps . . . . . 301**

Alexander Bienstock, *New York University*; Sarvar Patel and Joon Young Seo, *Google*; Kevin Yeo, *Google and Columbia University*

### **Distance-Aware Private Set Intersection . . . . . 319**

Anrin Chakraborti, *Duke University*; Giulia Fanti, *Carnegie Mellon University*; Michael K. Reiter, *Duke University*

### **Linear Private Set Union from Multi-Query Reverse Private Membership Test . . . . . 337**

Cong Zhang, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences*; Yu Chen, *School of Cyber Science and Technology, Shandong University; State Key Laboratory of Cryptology; Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University*; Weiran Liu, *Alibaba Group*; Min Zhang, *School of Cyber Science and Technology, Shandong University; State Key Laboratory of Cryptology; Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University*; Dongdai Lin, *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences*

## Logs and Auditing

### **Auditing Frameworks Need Resource Isolation: A Systematic Study on the Super Producer Threat to System Auditing and Its Mitigation . . . . . 355**

Peng Jiang, Ruizhe Huang, Ding Li, Yao Guo, and Xiangqun Chen, *MOE Key Lab of HCST, School of Computer Science, Peking University*; Jianhai Luan, Yuxin Ren, and Xinwei Hu, *Huawei Technologies*

### **AIRTAG: Towards Automated Attack Investigation by Unsupervised Learning with Log Texts . . . . . 373**

Hailun Ding, *Rutgers University*; Juan Zhai, *University of Massachusetts Amherst*; Yuhong Nan, *Sun Yat-sen University*; Shiqing Ma, *University of Massachusetts Amherst*

### **Rethinking System Audit Architectures for High Event Coverage and Synchronous Log Availability . . . . . 391**

Varun Gandhi, *Harvard University*; Sarbartha Banerjee, *University of Texas at Austin*; Aniket Agrawal and Adil Ahmad, *Arizona State University*; Sangho Lee and Marcus Peinado, *Microsoft Research*

### **Improving Logging to Reduce Permission Over-Granting Mistakes . . . . . 409**

Bingyu Shen, Tianyi Shan, and Yuanyuan Zhou, *University of California, San Diego*

## Fighting the Robots

- Dividing into Robocall Content with SnorCall** ..... 427  
Sathvik Prasad, Trevor Dunlap, Alexander Ross, and Bradley Reaves, *North Carolina State University*
- UCBlocker: Unwanted Call Blocking Using Anonymous Authentication** ..... 445  
Changlai Du and Hexuan Yu, *Virginia Tech*; Yang Xiao, *University of Kentucky*; Y. Thomas Hou, *Virginia Tech*;  
Angelos D. Keromytis, *Georgia Institute of Technology*; Wenjing Lou, *Virginia Tech*
- Combating Robocalls with Phone Virtual Assistant Mediated Interaction** ..... 463  
Sharbani Pandit, *Georgia Institute of Technology*; Krishanu Sarker, *Georgia State University*; Roberto Perdisci,  
*University of Georgia and Georgia Institute of Technology*; Mustaque Ahamad and Diyi Yang, *Georgia Institute  
of Technology*
- BotScreen: Trust Everybody, but Cut the Aimbots Yourself** ..... 481  
Minyeop Choi, *KAIST*; Gihyuk Ko, *Cyber Security Research Center at KAIST and Carnegie Mellon University*;  
Sang Kil Cha, *KAIST and Cyber Security Research Center at KAIST*

## Perspectives and Incentives

- “If I could do this, I feel anyone could:” The Design and Evaluation of a Secondary Authentication  
Factor Manager** ..... 499  
Garrett Smith, Tarun Yadav, and Jonathan Dutton, *Brigham Young University*; Scott Ruoti, *University of Tennessee Knoxville*;  
Kent Seamons, *Brigham Young University*
- Exploring Privacy and Incentives Considerations in Adoption of COVID-19 Contact Tracing Apps** ..... 517  
Oshrat Ayalon, *Max Planck Institute for Software Systems*; Dana Turjeman, *Reichman University*; Elissa M. Redmiles,  
*Max Planck Institute for Software Systems*
- Exploring Tenants’ Preferences of Privacy Negotiation in Airbnb** ..... 535  
Zixin Wang, *Zhejiang University*; Danny Yuxing Huang, *New York University*; Yaxing Yao, *University of Maryland,  
Baltimore County*
- Know Your Cybercriminal: Evaluating Attacker Preferences by Measuring Profile Sales on an Active,  
Leading Criminal Market for User Impersonation at Scale** ..... 553  
Michele Campobasso and Luca Allodi, *Eindhoven University of Technology*

## Traffic Analysis

- HorusEye: A Realtime IoT Malicious Traffic Detection Framework using Programmable Switches** ..... 571  
Yutao Dong, *Tsinghua Shenzhen International Graduate School, Shenzhen, China*; Peng Cheng Laboratory, *Shenzhen,  
China*; Qing Li, *Peng Cheng Laboratory, Shenzhen, China*; Kaidong Wu and Ruoyu Li, *Tsinghua Shenzhen International  
Graduate School, Shenzhen, China*; Peng Cheng Laboratory, *Shenzhen, China*; Dan Zhao, *Peng Cheng Laboratory,  
Shenzhen, China*; Gareth Tyson, *Hong Kong University of Science and Technology (GZ), Guangzhou, China*;  
Junkun Peng, Yong Jiang, and Shutao Xia, *Tsinghua Shenzhen International Graduate School, Shenzhen, China*;  
*Peng Cheng Laboratory, Shenzhen, China*; Mingwei Xu, *Tsinghua University, Beijing, China*
- An Input-Agnostic Hierarchical Deep Learning Framework for Traffic Fingerprinting** ..... 589  
Jian Qu, Xiaobo Ma, and Jianfeng Li, *Xi’an Jiaotong University*; Xiapu Luo, *The Hong Kong Polytechnic University*;  
Lei Xue, *Sun Yat-sen University*; Junjie Zhang, *Wright State University*; Zhenhua Li, *Tsinghua University*; Li Feng,  
*Southwest Jiaotong University*; Xiaohong Guan, *Xi’an Jiaotong University*
- Subverting Website Fingerprinting Defenses with Robust Traffic Representation** ..... 607  
Meng Shen, *School of Cyberspace Science and Technology, Beijing Institute of Technology*; Kexin Ji and Zhenbo Gao,  
*School of Computer Science, Beijing Institute of Technology*; Qi Li, *Institute for Network Sciences and Cyberspace,  
Tsinghua University*; Liehuang Zhu, *School of Cyberspace Science and Technology, Beijing Institute of Technology*;  
Ke Xu, *Department of Computer Science and Technology, Tsinghua University*
- Rosetta: Enabling Robust TLS Encrypted Traffic Classification in Diverse Network Environments  
with TCP-Aware Traffic Augmentation** ..... 625  
Renjie Xie and Jiahao Cao, *Tsinghua University*; Enhuan Dong and Mingwei Xu, *Tsinghua University and  
Quan Cheng Laboratory*; Kun Sun, *George Mason University*; Qi Li and Licheng Shen, *Tsinghua University*;  
Menghao Zhang, *Tsinghua University and Kuaishou Technology*

## Adversarial Patches and Images

- Towards Targeted Obfuscation of Adversarial Unsafe Images using Reconstruction and Counterfactual Super Region Attribution Explainability.** . . . . . 643  
Mazal Bethany, Andrew Seong, Samuel Henrique Silva, Nicole Beebe, Nishant Vishwamitra, and Peyman Najafirad, *The University of Texas at San Antonio*
- TPatch: A Triggered Physical Adversarial Patch** . . . . . 661  
Wenjun Zhu and Xiaoyu Ji, *USSLAB, Zhejiang University*; Yushi Cheng, *BNRist, Tsinghua University*; Shibo Zhang and Wenyan Xu, *USSLAB, Zhejiang University*
- CAPatch: Physical Adversarial Patch against Image Captioning Systems.** . . . . . 679  
Shibo Zhang, *USSLAB, Zhejiang University*; Yushi Cheng, *BNRist, Tsinghua University*; Wenjun Zhu, Xiaoyu Ji, and Wenyan Xu, *USSLAB, Zhejiang University*
- Hard-label Black-box Universal Adversarial Patch Attack** . . . . . 697  
Guanhong Tao, Shengwei An, Siyuan Cheng, Guangyu Shen, and Xiangyu Zhang, *Purdue University*

## Decentralized Finance

- Anatomy of a High-Profile Data Breach: Dissecting the Aftermath of a Crypto-Wallet Case.** . . . . . 715  
Svetlana Abramova and Rainer Böhme, *Universität Innsbruck*
- Glimpse: On-Demand PoW Light Client with Constant-Size Storage for DeFi.** . . . . . 733  
Giulia Scaffino, *TU Wien and Christian Doppler Laboratory Blockchain Technologies for the Internet of Things*; Lukas Aumayr and Zeta Avarikioti, *TU Wien*; Matteo Maffei, *TU Wien and Christian Doppler Laboratory Blockchain Technologies for the Internet of Things*
- Mixed Signals: Analyzing Ground-Truth Data on the Users and Economics of a Bitcoin Mixing Service** . . . . . 751  
Fieke Miedema, Kelvin Lubbertsen, Verena Schrama, and Rolf van Wegberg, *Delft University of Technology*
- Is Your Wallet Snitching On You? An Analysis on the Privacy Implications of Web3** . . . . . 769  
Christof Ferreira Torres, Fiona Willi, and Shweta Shinde, *ETH Zurich*

## Memory

- CAPSTONE: A Capability-based Foundation for Trustless Secure Memory Access** . . . . . 787  
Jason Zhijingcheng Yu, *National University of Singapore*; Conrad Watt, *University of Cambridge*; Aditya Badole, Trevor E. Carlson, and Prateek Saxena, *National University of Singapore*
- FloatZone: Accelerating Memory Error Detection using the Floating Point Unit.** . . . . . 805  
Floris Gorter, Enrico Barberis, Raphael Isemann, Erik van der Kouwe, Cristiano Giuffrida, and Herbert Bos, *Vrije Universiteit Amsterdam*
- PUMM: Preventing Use-After-Free Using Execution Unit Partitioning.** . . . . . 823  
Carter Yagemann, *The Ohio State University*; Simon P. Chung, Brendan Saltaformaggio, and Wenke Lee, *Georgia Institute of Technology*
- MTSan: A Feasible and Practical Memory Sanitizer for Fuzzing COTS Binaries** . . . . . 841  
Xingman Chen, *Tsinghua University*; Yinghao Shi, *Institute of Information Engineering, Chinese Academy of Sciences*; Zheyu Jiang and Yuan Li, *Tsinghua University*; Ruoyu Wang, *Arizona State University*; Haixin Duan, *Tsinghua University and Zhongguancun Laboratory*; Haoyu Wang, *Huazhong University of Science and Technology*; Chao Zhang, *Tsinghua University and Zhongguancun Laboratory*

## Security in Digital Realities

- Hidden Reality: Caution, Your Hand Gesture Inputs in the Immersive Virtual World are Visible to All!** . . . . . 859  
Sindhu Reddy Kalathur Gopal and Diksha Shukla, *University of Wyoming*; James David Wheelock, *University of Colorado Boulder*; Nitesh Saxena, *Texas A&M University, College Station*
- LocIn: Inferring Semantic Location from Spatial Maps in Mixed Reality** . . . . . 877  
Habiba Farrukh, Reham Mohamed, Aniket Nare, Antonio Bianchi, and Z. Berkay Celik, *Purdue University*

<b>Unique Identification of 50,000+ Virtual Reality Users from Head &amp; Hand Motion Data</b> .....	<b>895</b>
Vivek Nair and Wenbo Guo, <i>UC Berkeley</i> ; Justus Mattern, <i>RWTH Aachen</i> ; Rui Wang and James F. O'Brien, <i>UC Berkeley</i> ; Louis Rosenberg, <i>Unanimous AI</i> ; Dawn Song, <i>UC Berkeley</i>	
<b>Exploring User Reactions and Mental Models Towards Perceptual Manipulation Attacks in Mixed Reality</b> .....	<b>911</b>
Kaiming Cheng, Jeffery F. Tian, Tadayoshi Kohno, and Franziska Roesner, <i>University of Washington</i>	
<b>Erebus: Access Control for Augmented Reality Systems</b> .....	<b>929</b>
Yoonsang Kim, Sanket Goutam, Amir Rahmati, and Arie Kaufman, <i>Stony Brook University</i>	
<b>Password Guessing</b>	
<b>No Single Silver Bullet: Measuring the Accuracy of Password Strength Meters</b> .....	<b>947</b>
Ding Wang, Xuan Shan, and Qiying Dong, <i>Nankai University</i> ; Yaosheng Shen, <i>Peking University</i> ; Chunfu Jia, <i>Nankai University</i>	
<b>Password Guessing Using Random Forest</b> .....	<b>965</b>
Ding Wang and Yunkai Zou, <i>Nankai University</i> ; Zijian Zhang, <i>Peking University</i> ; Kedong Xiu, <i>Nankai University</i>	
<b>PASS2EDIT: A Multi-Step Generative Model for Guessing Edited Passwords</b> .....	<b>983</b>
Ding Wang and Yunkai Zou, <i>Nankai University</i> ; Yuan-An Xiao, <i>Peking University</i> ; Siqi Ma, <i>The University of New South Wales</i> ; Xiaofeng Chen, <i>Xidian University</i>	
<b>Improving Real-world Password Guessing Attacks via Bi-directional Transformers</b> .....	<b>1001</b>
Ming Xu and Jitao Yu, <i>Fudan University</i> ; Xinyi Zhang, <i>Facebook</i> ; Chuanwang Wang, Shenghao Zhang, Haoqi Wu, and Weili Han, <i>Fudan University</i>	
<b>Araña: Discovering and Characterizing Password Guessing Attacks in Practice</b> .....	<b>1019</b>
Mazharul Islam, <i>University of Wisconsin–Madison</i> ; Marina Sanusi Bohuk, <i>Cornell Tech</i> ; Paul Chung, <i>University of Wisconsin–Madison</i> ; Thomas Ristenpart, <i>Cornell Tech</i> ; Rahul Chatterjee, <i>University of Wisconsin–Madison</i>	
<b>Privacy Policies, Labels, Etc.</b>	
<b>POLIGRAPH: Automated Privacy Policy Analysis using Knowledge Graphs</b> .....	<b>1037</b>
Hao Cui, Rahmadi Trimananda, Athina Markopoulou, and Scott Jordan, <i>University of California, Irvine</i>	
<b>Calpric: Inclusive and Fine-grain Labeling of Privacy Policies with Crowdsourcing and Active Learning</b> .....	<b>1055</b>
Wenjun Qiu, David Lie, and Lisa Austin, <i>University of Toronto</i>	
<b>POLICYCOMP: Counterpart Comparison of Privacy Policies Uncovers Overbroad Personal Data Collection Practices</b> .....	<b>1073</b>
Lu Zhou, <i>Xidian University and Shanghai Jiao Tong University</i> ; Chengyongxiao Wei, Tong Zhu, and Guoxing Chen, <i>Shanghai Jiao Tong University</i> ; Xiaokuan Zhang, <i>George Mason University</i> ; Suguo Du, Hui Cao, and Haojin Zhu, <i>Shanghai Jiao Tong University</i>	
<b>Lalaine: Measuring and Characterizing Non-Compliance of Apple Privacy Labels</b> .....	<b>1091</b>
Yue Xiao, Zhengyi Li, and Yue Qin, <i>Indiana University Bloomington</i> ; Xiaolong Bai, <i>Orion Security Lab, Alibaba Group</i> ; Jiale Guan, Xiaojing Liao, and Luyi Xing, <i>Indiana University Bloomington</i>	
<b>Automated Cookie Notice Analysis and Enforcement</b> .....	<b>1109</b>
Rishabh Khandelwal and Asmit Nayak, <i>University of Wisconsin–Madison</i> ; Hamza Harkous, <i>Google, Inc.</i> ; Kassem Fawaz, <i>University of Wisconsin–Madison</i>	
<b>ML Applications to Malware</b>	
<b>Continuous Learning for Android Malware Detection</b> .....	<b>1127</b>
Yizheng Chen, Zhoujie Ding, and David Wagner, <i>UC Berkeley</i>	
<b>Humans vs. Machines in Malware Classification</b> .....	<b>1145</b>
Simone Aonzo, <i>EURECOM</i> ; Yufei Han, <i>INRIA</i> ; Alessandro Mantovani and Davide Balzarotti, <i>EURECOM</i>	
<b>Adversarial Training for Raw-Binary Malware Classifiers</b> .....	<b>1163</b>
Keane Lucas, Samruddhi Pai, Weiran Lin, and Lujo Bauer, <i>Carnegie Mellon University</i> ; Michael K. Reiter, <i>Duke University</i> ; Mahmood Sharif, <i>Tel Aviv University</i>	

**Black-box Adversarial Example Attack towards FCG Based Android Malware Detection under Incomplete Feature Information** . . . . . 1181  
Heng Li, *Huazhong University of Science and Technology*; Zhang Cheng, *NSFOCUS Technologies Group Co., Ltd. and Huazhong University of Science and Technology*; Bang Wu, Liheng Yuan, Cuiying Gao, and Wei Yuan, *Huazhong University of Science and Technology*; Xiapu Luo, *The Hong Kong Polytechnic University*

**Evading Provenance-Based ML Detectors with Adversarial System Actions** . . . . . 1199  
Kunal Mukherjee, Joshua Wiedemeier, Tianhao Wang, James Wei, Feng Chen, Muhyun Kim, Murat Kantarcioglu, and Kangkook Jee, *The University of Texas at Dallas*

## Secure Messaging

**TreeSync: Authenticated Group Management for Messaging Layer Security** . . . . . 1217  
Théophile Wallez, *Inria Paris*; Jonathan Protzenko, *Microsoft Research*; Benjamin Beurdouche, *Mozilla*; Karthikeyan Bhargavan, *Inria Paris*

**Formal Analysis of Session-Handling in Secure Messaging: Lifting Security from Sessions to Conversations** . . . . 1235  
Cas Cremers, *CISPA Helmholtz Center for Information Security*; Charlie Jacomme, *Inria Paris*; Aurora Naska, *CISPA Helmholtz Center for Information Security*

**Cryptographic Administration for Secure Group Messaging** . . . . . 1253  
David Balbás, *IMDEA Software Institute & Universidad Politécnica de Madrid*; Daniel Collins and Serge Vaudenay, *EPFL*

**Wink: Deniable Secure Messaging** . . . . . 1271  
Anrin Chakraborti, *Duke University*; Darius Suci and Radu Sion, *Stony Brook University*

**Three Lessons From Threema: Analysis of a Secure Messenger** . . . . . 1289  
Kenneth G. Paterson, Matteo Scarlata, and Kien Tuong Truong, *ETH Zurich*

## x-Fuzz

**MorFuzz: Fuzzing Processor via Runtime Instruction Morphing enhanced Synchronizable Co-simulation** . . . . 1307  
Jinyan Xu and Yiyuan Liu, *Zhejiang University*; Sirui He, *City University of Hong Kong*; Haoran Lin and Yajin Zhou, *Zhejiang University*; Cong Wang, *City University of Hong Kong*

**$\mu$ FUZZ: Redesign of Parallel Fuzzing using Microservice Architecture** . . . . . 1325  
Yongheng Chen, *Georgia Institute of Technology*; Rui Zhong, *Pennsylvania State University*; Yupeng Yang, *Georgia Institute of Technology*; Hong Hu and Dinghao Wu, *Pennsylvania State University*; Wenke Lee, *Georgia Institute of Technology*

**FISHFUZZ: Catch Deeper Bugs by Throwing Larger Nets** . . . . . 1343  
Han Zheng, *National Computer Network Intrusion Protection Center, University of Chinese Academy of Science; School of Computer and Communication Sciences, EPFL; Zhongguancun Laboratory*; Jiayuan Zhang, *National Computer Network Intrusion Protection Center, University of Chinese Academy of Science; School of Computer and Communication, Lanzhou University of Technology*; Yuhang Huang, *National Computer Network Intrusion Protection Center, University of Chinese Academy of Science*; Zezhong Ren, *National Computer Network Intrusion Protection Center, University of Chinese Academy of Science; Zhongguancun Laboratory*; He Wang, *School of Cyber Engineering, Xidian University*; Chunjie Cao, *School of Cyberspace Security, Hainan University*; Yuqing Zhang, *National Computer Network Intrusion Protection Center, University of Chinese Academy of Science; Zhongguancun Laboratory; School of Cyberspace Security, Hainan University; School of Cyber Engineering, Xidian University*; Flavio Toffalini and Mathias Payer, *School of Computer and Communication Sciences, EPFL*

**HyPFuzz: Formal-Assisted Processor Fuzzing** . . . . . 1361  
Chen Chen, Rahul Kande, Nathan Nguyen, Flemming Andersen, and Aakash Tyagi, *Texas A&M University*; Ahmad-Reza Sadeghi, *Technische Universität Darmstadt*; Jeyavijayan Rajendran, *Texas A&M University*

**POLYFUZZ: Holistic Greybox Fuzzing of Multi-Language Systems** . . . . . 1379  
Wen Li, Jinyang Ruan, and Guangbei Yi, *Washington State University*; Long Cheng, *Clemson University*; Xiapu Luo, *The Hong Kong Polytechnic University*; Haipeng Cai, *Washington State University*

## Programs, Code, and Binaries

**VIPER: Spotting Syscall-Guard Variables for Data-Only Attacks** ..... 1397  
Hengkai Ye, Song Liu, Zhechang Zhang, and Hong Hu, *The Pennsylvania State University*

**AURC: Detecting Errors in Program Code and Documentation** ..... 1415  
Peiwei Hu, Ruigang Liang, and Ying Cao, *SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, China, and School of Cyber Security, University of Chinese Academy of Sciences, China*; Kai Chen, *SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, China, School of Cyber Security, University of Chinese Academy of Sciences, China, and Beijing Academy of Artificial Intelligence, China*; Runze Zhang, *SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, China, and School of Cyber Security, University of Chinese Academy of Sciences, China*

**Not All Data are Created Equal: Data and Pointer Prioritization for Scalable Protection Against Data-Oriented Attacks** ..... 1433  
Salman Ahmed, *IBM Research*; Hans Liljestrand, *University of Waterloo*; Hani Jamjoom, *IBM Research*; Matthew Hicks, *Virginia Tech*; N. Asokan, *University of Waterloo*; Danfeng (Daphne) Yao, *Virginia Tech*

**SAFER: Efficient and Error-Tolerant Binary Instrumentation** ..... 1451  
Soumyakant Priyadarshan, Huan Nguyen, Rohit Chouhan, and R. Sekar, *Stony Brook University*

**Reassembly is Hard: A Reflection on Challenges and Strategies** ..... 1469  
Hyungseok Kim, *KAIST and The Affiliated Institute of ETRI*; Soomin Kim and Junoh Lee, *KAIST*; Kangkook Jee, *University of Texas at Dallas*; Sang Kil Cha, *KAIST*

## IoT Security Expectations and Barriers

**Measuring Up to (Reasonable) Consumer Expectations: Providing an Empirical Basis for Holding IoT Manufacturers Legally Responsible** ..... 1487  
Lorenz Kustosch and Carlos Gañán, *TU Delft*; Mattis van 't Schip, *Radboud University*; Michel van Eeten and Simon Parkin, *TU Delft*

**Are Consumers Willing to Pay for Security and Privacy of IoT Devices?** ..... 1505  
Pardis Emami-Naeini, *Duke University*; Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor, *Carnegie Mellon University*

**Examining Consumer Reviews to Understand Security and Privacy Issues in the Market of Smart Home Devices** . . 1523  
Swaathi Vetrivel, Veerle van Harten, Carlos H. Gañán, Michel van Eeten, and Simon Parkin, *Delft University of Technology*

**Internet Service Providers' and Individuals' Attitudes, Barriers, and Incentives to Secure IoT** ..... 1541  
Nissy Sombatruang, *National Institute of Information and Communications Technology*; Tristan Caulfield and Ingolf Becker, *University College London*; Akira Fujita, Takahiro Kasama, Koji Nakao, and Daisuke Inoue, *National Institute of Information and Communications Technology*

**Detecting and Handling IoT Interaction Threats in Multi-Platform Multi-Control-Channel Smart Homes** . . . . . 1559  
Haotian Chi, *Shanxi University and Temple University*; Qiang Zeng, *George Mason University*; Xiaojiang Du, *Stevens Institute of Technology*

## Differential Privacy

**Private Proof-of-Stake Blockchains using Differentially-Private Stake Distortion** ..... 1577  
Chenghong Wang, David Pujol, Kartik Nayak, and Ashwin Machanavajjhala, *Duke University*

**PRIVATEFL: Accurate, Differentially Private Federated Learning via Personalized Data Transformation** ..... 1595  
Yuchen Yang, Bo Hui, and Haolin Yuan, *The Johns Hopkins University*; Neil Gong, *Duke University*; Yinzhi Cao, *The Johns Hopkins University*

**What Are the Chances? Explaining the Epsilon Parameter in Differential Privacy** ..... 1613  
Priyanka Nanayakkara, *Northwestern University*; Mary Anne Smart, *University of California San Diego*; Rachel Cummings, *Columbia University*; Gabriel Kaptchuk, *Boston University*; Elissa M. Redmiles, *Max Planck Institute for Software Systems*

<b>Tight Auditing of Differentially Private Machine Learning</b> .....	<b>1631</b>
Milad Nasr, Jamie Hayes, Thomas Steinke, and Borja Balle, <i>Google DeepMind</i> ; Florian Tramèr, <i>ETH Zurich</i> ; Matthew Jagielski, Nicholas Carlini, and Andreas Terzis, <i>Google DeepMind</i>	
<b>PrivTrace: Differentially Private Trajectory Synthesis by Adaptive Markov Models</b> .....	<b>1649</b>
Haiming Wang, <i>Zhejiang University</i> ; Zhikun Zhang, <i>CISPA Helmholtz Center for Information Security</i> ; Tianhao Wang, <i>University of Virginia</i> ; Shibo He, <i>Zhejiang University</i> ; Michael Backes, <i>CISPA Helmholtz Center for Information Security</i> ; Jiming Chen, <i>Zhejiang University</i> ; Yang Zhang, <i>CISPA Helmholtz Center for Information Security</i>	
<b>Poisoning</b>	
<b>META-SIFT: How to Sift Out a Clean Subset in the Presence of Data Poisoning?</b> .....	<b>1667</b>
Yi Zeng, <i>Virginia Tech and SONY AI</i> ; Minzhou Pan, Himanshu Jahagirdar, and Ming Jin, <i>Virginia Tech</i> ; Lingjuan Lyu, <i>SONY AI</i> ; Ruoxi Jia, <i>Virginia Tech</i>	
<b>Towards A Proactive ML Approach for Detecting Backdoor Poison Samples</b> .....	<b>1685</b>
Xiangyu Qi, Tinghao Xie, Jiachen T. Wang, Tong Wu, Saeed Mahloujifar, and Prateek Mittal, <i>Princeton University</i>	
<b>PORE: Provably Robust Recommender Systems against Data Poisoning Attacks</b> .....	<b>1703</b>
Jinyuan Jia, <i>The Pennsylvania State University</i> ; Yupei Liu, Yuepeng Hu, and Neil Zhenqiang Gong, <i>Duke University</i>	
<b>Every Vote Counts: Ranking-Based Training of Federated Learning to Resist Poisoning Attacks</b> .....	<b>1721</b>
Hamid Mozaffari, Virat Shejwalkar, and Amir Houmansadr, <i>University of Massachusetts Amherst</i>	
<b>Fine-grained Poisoning Attack to Local Differential Privacy Protocols for Mean and Variance Estimation</b> .....	<b>1739</b>
Xiaoguang Li, <i>Xidian University and Purdue University</i> ; Ninghui Li and Wenhai Sun, <i>Purdue University</i> ; Neil Zhenqiang Gong, <i>Duke University</i> ; Hui Li, <i>Xidian University</i>	
<b>Smart Contracts</b>	
<b>Your Exploit is Mine: Instantly Synthesizing Counterattack Smart Contract</b> .....	<b>1757</b>
Zhuo Zhang, <i>Purdue University</i> ; Zhiqiang Lin and Marcelo Morales, <i>Ohio State University</i> ; Xiangyu Zhang and Kaiyuan Zhang, <i>Purdue University</i>	
<b>Smart Learning to Find Dumb Contracts</b> .....	<b>1775</b>
Tamer Abdelaziz, <i>National University of Singapore</i> ; Aquinas Hobor, <i>University College London</i>	
<b>Confusum Contractum: Confused Deputy Vulnerabilities in Ethereum Smart Contracts</b> .....	<b>1793</b>
Fabio Gritti, Nicola Ruaro, Robert McLaughlin, Priyanka Bose, Dipanjan Das, Ilya Grishchenko, Christopher Kruegel, and Giovanni Vigna, <i>University of California, Santa Barbara</i>	
<b>Panda: Security Analysis of Algorand Smart Contracts</b> .....	<b>1811</b>
Zhiyuan Sun, <i>The Hong Kong Polytechnic University and Southern University of Science and Technology</i> ; Xiapu Luo, <i>The Hong Kong Polytechnic University</i> ; Yinqian Zhang, <i>Southern University of Science and Technology</i>	
<b>Proxy Hunting: Understanding and Characterizing Proxy-based Upgradeable Smart Contracts in Blockchains</b> ..	<b>1829</b>
William E Bodell III, Sajad Meisami, and Yue Duan, <i>Illinois Institute of Technology</i>	
<b>x-Fuzz and Fuzz-x</b>	
<b>Fuzztruction: Using Fault Injection-based Fuzzing to Leverage Implicit Domain Knowledge</b> .....	<b>1847</b>
Nils Bars, Moritz Schloegel, Tobias Scharnowski, and Nico Schiller, <i>Ruhr-Universität Bochum</i> ; Thorsten Holz, <i>CISPA Helmholtz Center for Information Security</i>	
<b>FuzzJIT: Oracle-Enhanced Fuzzing for JavaScript Engine JIT Compiler</b> .....	<b>1865</b>
Junjie Wang, <i>College of Intelligence and Computing, Tianjin University</i> ; Zhiyi Zhang, <i>CodeSafe Team</i> , <i>Qi An Xin Group Corp.</i> ; Shuang Liu, <i>College of Intelligence and Computing, Tianjin University</i> ; Xiaoning Du, <i>Monash University</i> ; Junjie Chen, <i>College of Intelligence and Computing, Tianjin University</i>	
<b>GLeeFuzz: Fuzzing WebGL Through Error Message Guided Mutation</b> .....	<b>1883</b>
Hui Peng, <i>Purdue University</i> ; Zhihao Yao and Ardalan Amiri Sani, <i>UC Irvine</i> ; Dave (Jing) Tian, <i>Purdue University</i> ; Mathias Payer, <i>EPFL</i>	



<b>autofz: Automated Fuzzer Composition at Runtime</b> .....	<b>1901</b>
Yu-Fu Fu, Jaehyuk Lee, and Taesoo Kim, <i>Georgia Institute of Technology</i>	
<b>CarpetFuzz: Automatic Program Option Constraint Extraction from Documentation for Fuzzing</b> .....	<b>1919</b>
Dawei Wang, Ying Li, and Zhiyu Zhang, <i>SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China</i> ; Kai Chen, <i>SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China; Beijing Academy of Artificial Intelligence, China</i>	
<b>Cache Attacks</b>	
<b>SCARF – A Low-Latency Block Cipher for Secure Cache-Randomization</b> .....	<b>1937</b>
Federico Canale, <i>Ruhr-University Bochum</i> ; Tim Güneysu, <i>Ruhr-University Bochum and DFKI</i> ; Gregor Leander and Jan Philipp Thoma, <i>Ruhr-University Bochum</i> ; Yosuke Todo, <i>NTT Social Informatics Laboratories</i> ; Rei Ueno, <i>Tohoku University</i>	
<b>The Gates of Time: Improving Cache Attacks with Transient Execution</b> .....	<b>1955</b>
Daniel Katzman, <i>Tel Aviv University</i> ; William Kosasih, <i>The University of Adelaide</i> ; Chitchanok Chuengsatiansup, <i>The University of Melbourne</i> ; Eyal Ronen, <i>Tel Aviv University</i> ; Yuval Yarom, <i>The University of Adelaide</i>	
<b>Synchronization Storage Channels (S<sup>2</sup>C): Timer-less Cache Side-Channel Attacks on the Apple M1 via Hardware Synchronization Instructions</b> .....	<b>1973</b>
Jiyong Yu and Aishani Dutta, <i>University of Illinois Urbana-Champaign</i> ; Trent Jaeger, <i>Pennsylvania State University</i> ; David Kohlbrenner, <i>University of Washington</i> ; Christopher W. Fletcher, <i>University of Illinois Urbana-Champaign</i>	
<b>CLEPSYDRACACHE – Preventing Cache Attacks with Time-Based Evictions</b> .....	<b>1991</b>
Jan Philipp Thoma, <i>Ruhr University Bochum</i> ; Christian Niesler, <i>University of Duisburg-Essen</i> ; Dominic Funke, Gregor Leander, Pierre Mayr, and Nils Pohl, <i>Ruhr University Bochum</i> ; Lucas Davi, <i>University of Duisburg-Essen</i> ; Tim Güneysu, <i>Ruhr University Bochum &amp; DFKI</i>	
<b>CACHEQL: Quantifying and Localizing Cache Side-Channel Vulnerabilities in Production Software</b> .....	<b>2009</b>
Yuan Yuan, Zhibo Liu, and Shuai Wang, <i>The Hong Kong University of Science and Technology</i>	
<b>Authentication</b>	
<b>InfinityGauntlet: Expose Smartphone Fingerprint Authentication to Brute-force Attack</b> .....	<b>2027</b>
Yu Chen and Yang Yu, <i>Xuanwu Lab, Tencent</i> ; Lidong Zhai, <i>Institute of Information Engineering, Chinese Academy of Sciences</i>	
<b>A Study of Multi-Factor and Risk-Based Authentication Availability</b> .....	<b>2043</b>
Anthony Gavazzi, Ryan Williams, Engin Kirda, and Long Lu, <i>Northeastern University</i> ; Andre King, Andy Davis, and Tim Leek, <i>MIT Lincoln Laboratory</i>	
<b>A Large-Scale Measurement of Website Login Policies</b> .....	<b>2061</b>
Suood Al Roomi, <i>Georgia Institute of Technology, Kuwait University</i> ; Frank Li, <i>Georgia Institute of Technology</i>	
<b>Security and Privacy Failures in Popular 2FA Apps</b> .....	<b>2079</b>
Conor Gilsean, <i>UC Berkeley / ICSI</i> ; Fuzail Shakir and Noura Alomar, <i>UC Berkeley</i> ; Serge Egelman, <i>UC Berkeley / ICSI</i>	
<b>Multi-Factor Key Derivation Function (MFKDF) for Fast, Flexible, Secure, &amp; Practical Key Management</b> .....	<b>2097</b>
Vivek Nair and Dawn Song, <i>University of California, Berkeley</i>	
<b>Private Data Leaks</b>	
<b>Log: It's Big, It's Heavy, It's Filled with Personal Data! Measuring the Logging of Sensitive Information in the Android Ecosystem</b> .....	<b>2115</b>
Allan Lyons, <i>University of Calgary</i> ; Julien Gamba, <i>IMDEA Networks Institute and Universidad Carlos III de Madrid</i> ; Austin Shawaga, <i>University of Calgary</i> ; Joel Reardon, <i>University of Calgary and AppCensus, Inc.</i> ; Juan Tapiador, <i>Universidad Carlos III de Madrid</i> ; Serge Egelman, <i>ICSI and UC Berkeley and AppCensus, Inc.</i> ; Narseo Vallina-Rodriguez, <i>IMDEA Networks Institute and AppCensus, Inc.</i>	
<b>CodexLeaks: Privacy Leaks from Code Generation Language Models in GitHub Copilot</b> .....	<b>2133</b>
Liang Niu and Shujaat Mirza, <i>New York University</i> ; Zayd Maradni and Christina Pöpper, <i>New York University Abu Dhabi</i>	

**Freaky Leaky SMS: Extracting User Locations by Analyzing SMS Timings** ..... 2151  
Evangelos Bitsikas, *Northeastern University*; Theodor Schnitzler, *Research Center Trustworthy Data Science and Security*;  
Christina Pöpper, *New York University Abu Dhabi*; Aanjhan Ranganathan, *Northeastern University*

**The Writing on the Wall and 3D Digital Twins: Personal Information in (not so) Private Real Estate** ..... 2169  
Rachel McAmis and Tadayoshi Kohno, *University of Washington*

## **Generative AI**

**Glaze: Protecting Artists from Style Mimicry by Text-to-Image Models**..... 2187  
Shawn Shan, Jenna Cryan, Emily Wenger, Haitao Zheng, Rana Hanocka, and Ben Y. Zhao, *University of Chicago*

**Lost at C: A User Study on the Security Implications of Large Language Model Code Assistants**..... 2205  
Gustavo Sandoval, Hammond Pearce, Teo Nys, Ramesh Karri, Siddharth Garg, and Brendan Dolan-Gavitt,  
*New York University*

**Two-in-One: A Model Hijacking Attack Against Text Generation Models** ..... 2223  
Wai Man Si, Michael Backes, and Yang Zhang, *CISPA Helmholtz Center for Information Security*; Ahmed Salem, *Microsoft*

**PTW: Pivotal Tuning Watermarking for Pre-Trained Image Generators** ..... 2241  
Nils Lukas and Florian Kerschbaum, *University of Waterloo*

## **Security Worker Perspectives**

**Lessons Lost: Incident Response in the Age of Cyber Insurance and Breach Attorneys** ..... 2259  
Daniel W. Woods, *University of Edinburgh*; Rainer Böhme, *University of Innsbruck*; Josephine Wolff, *Tufts University*;  
Daniel Schwarcz, *University of Minnesota*

**Bug Hunters' Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem**..... 2275  
Omer Akgul, *University of Maryland*; Taha Eghtesad, *Pennsylvania State University*; Amit Elazari, *University of California, Berkeley*;  
Omprakash Gnawali, *University of Houston*; Jens Grossklags, *Technical University of Munich*;  
Michelle L. Mazurek, *University of Maryland*; Daniel Votipka, *Tufts University*; Aron Laszka, *Pennsylvania State University*

**Work-From-Home and COVID-19: Trajectories of Endpoint Security Management in a Security Operations Center**..... 2293  
Kailani R. Jones and Dalton A. Brucker-Hahn, *University of Kansas*; Bradley Fidler, *Independent Researcher*;  
Alexandru G. Bardas, *University of Kansas*

**“Employees Who Don’t Accept the Time Security Takes Are Not Aware Enough”: The CISO View of Human-Centred Security**..... 2311  
Jonas Hielscher and Uta Menges, *Ruhr University Bochum*; Simon Parkin, *TU Delft*; Annette Kluge and M. Angela Sasse,  
*Ruhr University Bochum*

## **Deep Thoughts on Deep Learning**

**Aegis: Mitigating Targeted Bit-flip Attacks against Deep Neural Networks** ..... 2329  
Jialai Wang, *Tsinghua University*; Ziyuan Zhang, *Beijing University of Posts and Telecommunications*; Meiqi Wang,  
*Tsinghua University*; Han Qiu, *Tsinghua University and Zhongguancun Laboratory*; Tianwei Zhang, *Nanyang Technological University*;  
Qi Li, *Tsinghua University and Zhongguancun Laboratory*; Zongpeng Li, *Tsinghua University and Hangzhou Dianzi University*;  
Tao Wei, *Ant Group*; Chao Zhang, *Tsinghua University and Zhongguancun Laboratory*

**Rethinking White-Box Watermarks on Deep Learning Models under Neural Structural Obfuscation**..... 2347  
Yifan Yan, Xudong Pan, Mi Zhang, and Min Yang, *Fudan University*

**PELICAN: Exploiting Backdoors of Naturally Trained Deep Learning Models In Binary Code Analysis** ..... 2365  
Zhuo Zhang, Guanhong Tao, Guangyu Shen, Shengwei An, Qiuling Xu, Yingqi Liu, and Yapeng Ye, *Purdue University*;  
Yaoyuan Wu, *University of California, Los Angeles*; Xiangyu Zhang, *Purdue University*

**IvySyn: Automated Vulnerability Discovery in Deep Learning Frameworks** ..... 2383  
Neophytos Christou, Di Jin, and Vaggelis Atlidakis, *Brown University*; Baishakhi Ray, *Columbia University*;  
Vasileios P. Kemerlis, *Brown University*

## Thursday, August 10

### Smart? Assistants

**Hey Kimya, Is My Smart Speaker Spying on Me? Taking Control of Sensor Privacy Through Isolation and Amnesia** ..... 2401  
Piet De Vaere and Adrian Perrig, *ETH Zürich*

**Spying through Your Voice Assistants: Realistic Voice Command Fingerprinting** ..... 2419  
Dilawer Ahmed, Aafaq Sabir, and Anupam Das, *North Carolina State University*

**QFA2SR: Query-Free Adversarial Transfer Attacks to Speaker Recognition Systems** ..... 2437  
Guangke Chen, Yedi Zhang, and Zhe Zhao, *ShanghaiTech University*; Fu Song, *ShanghaiTech University*; *Automotive Software Innovation Center*; *Institute of Software, Chinese Academy of Sciences & University of Chinese Academy of Sciences*

**Learning Normality is Enough: A Software-based Mitigation against Inaudible Voice Attacks** ..... 2455  
Xinfeng Li, Xiaoyu Ji, and Chen Yan, *USSLAB, Zhejiang University*; Chao hao Li, *USSLAB, Zhejiang University and Hangzhou Hikvision Digital Technology Co., Ltd.*; Yichen Li, *Hong Kong University of Science and Technology*; Zhenning Zhang, *University of Illinois at Urbana-Champaign*; Wenyuan Xu, *USSLAB, Zhejiang University*

**Powering for Privacy: Improving User Trust in Smart Speaker Microphones with Intentional Powering and Perceptible Assurance** ..... 2473  
Youngwook Do and Nivedita Arora, *Georgia Institute of Technology*; Ali Mirzazadeh and Injoo Moon, *Georgia Institute of Technology and Massachusetts Institute of Technology*; Eryue Xu, *Georgia Institute of Technology*; Zhihan Zhang, *Georgia Institute of Technology and University of Washington*; Gregory D. Abowd, *Georgia Institute of Technology and Northeastern University*; Sauvik Das, *Georgia Institute of Technology and Carnegie Mellon University*

### Security-Adjacent Worker Perspectives

**To Cloud or not to Cloud: A Qualitative Study on Self-Hosters' Motivation, Operation, and Security Mindset** ... 2491  
Lea Gröber, *CISPA Helmholtz Center for Information Security and Saarland University*; Rafael Mrowczynski, *CISPA Helmholtz Center for Information Security*; Nimisha Vijay and Daphne A. Muller, *Nextcloud*; Adrian Dabrowski and Katharina Krombholz, *CISPA Helmholtz Center for Information Security*

**"I wouldn't want my unsafe code to run my pacemaker": An Interview Study on the Use, Comprehension, and Perceived Risks of Unsafe Rust** ..... 2509  
Sandra Höltervennhoff, *Leibniz University Hannover*; Philip Klostermeyer and Noah Wöhler, *CISPA Helmholtz Center for Information Security*; Yasemin Acar, *Paderborn University, George Washington University*; Sascha Fahl, *CISPA Helmholtz Center for Information Security*

**Pushed by Accident: A Mixed-Methods Study on Strategies of Handling Secret Information in Source Code Repositories** ..... 2527  
Alexander Krause, *CISPA Helmholtz Center for Information Security*; Jan H. Klemmer and Nicolas Huaman, *Leibniz University Hannover*; Dominik Wermke, *CISPA Helmholtz Center for Information Security*; Yasemin Acar, *Paderborn University, George Washington University*; Sascha Fahl, *CISPA Helmholtz Center for Information Security*

**A Mixed-Methods Study of Security Practices of Smart Contract Developers** ..... 2545  
Tanusree Sharma, Zhixuan Zhou, Andrew Miller, and Yang Wang, *University of Illinois at Urbana Champaign*

**The Role of Professional Product Reviewers in Evaluating Security and Privacy** ..... 2563  
Wentao Guo, Jason Walter, and Michelle L. Mazurek, *University of Maryland*

### Censorship and Internet Freedom

**Network Responses to Russia's Invasion of Ukraine in 2022: A Cautionary Tale for Internet Freedom** ..... 2581  
Reethika Ramesh, Ram Sundara Raman, and Apurva Virkud, *University of Michigan*; Alexandra Dirksen, *TU Braunschweig*; Armin Huremagic, *University of Michigan*; David Fifield, *unaffiliated*; Dirk Rodenburg and Rod Hynes, *Psiphon*; Doug Madory, *Kentik*; Roya Ensafi, *University of Michigan*

**A Study of China's Censorship and Its Evasion Through the Lens of Online Gaming** ..... 2599  
Yuzhou Feng, *Florida International University*; Ruyi Zhai, *Hangzhou Dianzi University*; Radu Sion, *Stony Brook University*; Bogdan Carbutar, *Florida International University*

**DeResistor: Toward Detection-Resistant Probing for Evasion of Internet Censorship** . . . . . 2617  
Abderrahmen Amich and Birhanu Eshete, *University of Michigan, Dearborn*; Vinod Yegneswaran, *SRI International*;  
Nguyen Phong Hoang, *University of Chicago*

**Timeless Timing Attacks and Preload Defenses in Tor’s DNS Cache** . . . . . 2635  
Rasmus Dahlberg and Tobias Pulls, *Karlstad University*

**How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic** . . . . . 2653  
Mingshi Wu, *GFW Report*; Jackson Sippe, *University of Colorado Boulder*; Danesh Sivakumar and Jack Burg,  
*University of Maryland*; Peter Anderson, *Independent researcher*; Xiaokang Wang, *V2Ray Project*; Kevin Bock,  
*University of Maryland*; Amir Houmansadr, *University of Massachusetts Amherst*; Dave Levin, *University of Maryland*;  
Eric Wustrow, *University of Colorado Boulder*

## Machine Learning Backdoors

**A Data-free Backdoor Injection Approach in Neural Networks** . . . . . 2671  
Peizhuo Lv, Chang Yue, Ruigang Liang, and Yunfei Yang, *SKLOIS, Institute of Information Engineering,  
Chinese Academy of Sciences, China*; *School of Cyber Security, University of Chinese Academy of Sciences, China*;  
Shengzhi Zhang, *Department of Computer Science, Metropolitan College, Boston University, USA*; Hualong Ma,  
*SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, China*; *School of Cyber Security,  
University of Chinese Academy of Sciences, China*; Kai Chen, *SKLOIS, Institute of Information Engineering,  
Chinese Academy of Sciences, China*; *School of Cyber Security, University of Chinese Academy of Sciences, China*;  
*Beijing Academy of Artificial Intelligence, China*

**Sparsity Brings Vulnerabilities: Exploring New Metrics in Backdoor Attacks** . . . . . 2689  
Jianwen Tian, *NKLSTISS, Institute of Systems Engineering, Academy of Military Sciences, China*; Kefan Qiu, *School of  
Cyberspace Science and Technology, Beijing Institute of Technology*; Debin Gao, *Singapore Management University*;  
Zhi Wang, *DISSec, College of Cyber Science, Nankai University*; Xiaohui Kuang and Gang Zhao, *NKLSTISS, Institute of  
Systems Engineering, Academy of Military Sciences, China*

**Aliasing Backdoor Attacks on Pre-trained Models** . . . . . 2707  
Cheng’an Wei, *SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, China*; *School of  
Cyber Security, University of Chinese Academy of Sciences, China*; Yeonjoon Lee, *Hanyang University, Ansan,  
Republic of Korea*; Kai Chen, Guozhu Meng, and Peizhuo Lv, *SKLOIS, Institute of Information Engineering,  
Chinese Academy of Sciences, China*; *School of Cyber Security, University of Chinese Academy of Sciences, China*

**ASSET: Robust Backdoor Data Detection Across a Multiplicity of Deep Learning Paradigms** . . . . . 2725  
Minzhou Pan and Yi Zeng, *Virginia Tech*; Lingjuan Lyu, *Sony AI*; Xue Lin, *Northeastern University*; Ruoxi Jia,  
*Virginia Tech*

**VILLAIN: Backdoor Attacks Against Vertical Split Learning** . . . . . 2743  
Yijie Bai and Yanjiao Chen, *Zhejiang University*; Hanlei Zhang and Wenyan Xu, *Zhejiang University*; Haiqin Weng  
and Dou Goodman, *Ant Group*

## Integrity

**ARI: Attestation of Real-time Mission Execution Integrity** . . . . . 2761  
Jinwen Wang, Yujie Wang, and Ao Li, *Washington University in St. Louis*; Yang Xiao, *University of Kentucky*;  
Ruide Zhang, Wenjing Lou, and Y. Thomas Hou, *Virginia Polytechnic Institute and State University*; Ning Zhang,  
*Washington University in St. Louis*

**Design of Access Control Mechanisms in Systems-on-Chip with Formal Integrity Guarantees** . . . . . 2779  
Dino Mehmedagić, Mohammad Rahmani Fadiheh, Johannes Müller, Anna Lena Duque Antón, Dominik Stoffel,  
and Wolfgang Kunz, *Rheinland-Pfälzische Technische Universität (RPTU) Kaiserslautern-Landau, Germany*

**HashTag: Hash-based Integrity Protection for Tagged Architectures** . . . . . 2797  
Lukas Lamster, Martin Unterguggenberger, David Schrammel, and Stefan Mangard, *Graz University of Technology*

**XCheck: Verifying Integrity of 3D Printed Patient-Specific Devices via Computing Tomography** . . . . . 2815  
Zhiyuan Yu, Yuanhaur Chang, Shixuan Zhai, Nicholas Deily, and Tao Ju, *Washington University in St. Louis*;  
XiaoFeng Wang, *Indiana University Bloomington*; Uday Jammalamadaka, *Rice University*; Ning Zhang,  
*Washington University in St. Louis*

**Demystifying Pointer Authentication on Apple M1** . . . . . 2833  
Zechao Cai, Jiaxun Zhu, Wenbo Shen, Yutian Yang, and Rui Chang, *Zhejiang University and ZJU-Hangzhou Global Scientific and Technological Innovation Center*; Yu Wang, *Hangzhou Cyberserval Co., Ltd.*; Jinku Li, *Xidian University*; Kui Ren, *Zhejiang University and ZJU-Hangzhou Global Scientific and Technological Innovation Center*

## Fuzzing Firmware and Drivers

**DDRace: Finding Concurrency UAF Vulnerabilities in Linux Drivers with Directed Fuzzing** . . . . . 2849  
Ming Yuan and Bodong Zhao, *Tsinghua University*; Penghui Li, *The Chinese University of Hong Kong*; Jiashuo Liang and Xinhui Han, *Peking University*; Xiapu Luo, *The Hong Kong Polytechnic University*; Chao Zhang, *Tsinghua University and Zhongguancun Lab*

**Automata-Guided Control-Flow-Sensitive Fuzz Driver Generation** . . . . . 2867  
Cen Zhang and Yuekang Li, *Nanyang Technological University, Continental-NTU Corporate Lab*; Hao Zhou, *The Hong Kong Polytechnic University*; Xiaohan Zhang, *Xidian University*; Yaowen Zheng, *Nanyang Technological University, Continental-NTU Corporate Lab*; Xian Zhan, *Southern University of Science and Technology*; *The Hong Kong Polytechnic University*; Xiaofei Xie, *Singapore Management University*; Xiapu Luo, *The Hong Kong Polytechnic University*; Xinghua Li, *Xidian University*; Yang Liu, *Nanyang Technological University, Continental-NTU Corporate Lab*; Sheikh Mahbub Habib, *Continental AG, Germany*

**HOEDUR: Embedded Firmware Fuzzing using Multi-Stream Inputs** . . . . . 2885  
Tobias Scharnowski and Simon Wörner, *CISPA Helmholtz Center for Information Security*; Felix Buchmann, *Ruhr University Bochum*; Nils Bars, Moritz Schloegel, and Thorsten Holz, *CISPA Helmholtz Center for Information Security*

**Forming Faster Firmware Fuzzers** . . . . . 2903  
Lukas Seidel, *Qwiet AI*; Dominik Maier, *TU Berlin*; Marius Muench, *VU Amsterdam and University of Birmingham*

**ReUSB: Replay-Guided USB Driver Fuzzing** . . . . . 2921  
Jisoo Jang, Minsuk Kang, and Dokyung Song, *Yonsei University*

## Vehicles and Security

**Exorcising “Wraith”: Protecting LiDAR-based Object Detector in Automated Driving System from Appearing Attacks** . . . . . 2939  
Qifan Xiao, Xudong Pan, Yifan Lu, Mi Zhang, Jiarun Dai, and Min Yang, *Fudan University*

**Discovering Adversarial Driving Maneuvers against Autonomous Vehicles** . . . . . 2957  
Ruoyu Song, Muslum Ozgur Ozmen, Hyungsub Kim, Raymond Muller, Z. Berkay Celik, and Antonio Bianchi, *Purdue University*

**Understand Users’ Privacy Perception and Decision of V2X Communication in Connected Autonomous Vehicles** . . . 2975  
Zekun Cai and Aiping Xiong, *The Pennsylvania State University*

**You Can’t See Me: Physical Removal Attacks on LiDAR-based Autonomous Vehicles Driving Frameworks** . . . . . 2993  
Yulong Cao, *University of Michigan*; S. Hrushikesh Bhupathiraju and Pirouz Naghavi, *University of Florida*; Takeshi Sugawara, *The University of Electro-Communications*; Z. Morley Mao, *University of Michigan*; Sara Rampazzi, *University of Florida*

**PatchVerif: Discovering Faulty Patches in Robotic Vehicles** . . . . . 3011  
Hyungsub Kim, Muslum Ozgur Ozmen, Z. Berkay Celik, Antonio Bianchi, and Dongyan Xu, *Purdue University*

## Verifying Users

**Fast IDentity Online with Anonymous Credentials (FIDO-AC)** . . . . . 3029  
Wei-Zhu Yeoh, *CISPA Helmholtz Center for Information Security*; Michal Kepkowski, *Macquarie University*; Gunnar Heide, *CISPA Helmholtz Center for Information Security*; Dali Kaafar, *Macquarie University*; Lucjan Hanzlik, *CISPA Helmholtz Center for Information Security*

**How to Bind Anonymous Credentials to Humans** . . . . . 3047  
Julia Hesse, *IBM Research Europe - Zurich*; Nitin Singh, *IBM Research India - Bangalore*; Alessandro Sorniotti, *IBM Research Europe - Zurich*

<b>Inducing Authentication Failures to Bypass Credit Card PINs</b> .....	<b>3065</b>
David Basin, Patrick Schaller, and Jorge Toro-Pozo, <i>ETH Zurich</i>	
<b>An Empirical Study &amp; Evaluation of Modern CAPTCHAs</b> .....	<b>3081</b>
Andrew Searles, <i>University of California, Irvine</i> ; Yoshimichi Nakatsuka, <i>ETH Zürich</i> ; Ercan Ozturk, <i>University of California, Irvine</i> ; Andrew Paverd, <i>Microsoft</i> ; Gene Tsudik, <i>University of California, Irvine</i> ; Ai Enkoji, <i>Lawrence Livermore National Laboratory</i>	
<b>Account Verification on Social Media: User Perceptions and Paid Enrollment</b> .....	<b>3099</b>
Madelyne Xiao, Mona Wang, Anunay Kulshrestha, and Jonathan Mayer, <i>Princeton University</i>	
<b>DNS Security</b>	
<b>User Awareness and Behaviors Concerning Encrypted DNS Settings in Web Browsers</b> .....	<b>3117</b>
Alexandra Nisenoff, <i>Carnegie Mellon University and University of Chicago</i> ; Ranya Sharma and Nick Feamster, <i>University of Chicago</i>	
<b>Two Sides of the Shield: Understanding Protective DNS adoption factors</b> .....	<b>3135</b>
Elsa Rodríguez, Radu Anghel, Simon Parkin, Michel van Eeten, and Carlos Gañán, <i>Delft University of Technology</i>	
<b>The Maginot Line: Attacking the Boundary of DNS Caching Protection</b> .....	<b>3153</b>
Xiang Li, Chaoyi Lu, and Baojun Liu, <i>Tsinghua University</i> ; Qifan Zhang and Zhou Li, <i>University of California, Irvine</i> ; Haixin Duan, <i>Tsinghua University, QI-ANXIN Technology Research Institute, and Zhongguancun Laboratory</i> ; Qi Li, <i>Tsinghua University and Zhongguancun Laboratory</i>	
<b>Fourteen Years in the Life: A Root Server’s Perspective on DNS Resolver Security</b> .....	<b>3171</b>
Alden Hilton, <i>Sandia National Laboratories</i> ; Casey Deccio, <i>Brigham Young University</i> ; Jacob Davis, <i>Sandia National Laboratories</i>	
<b>NRDelegationAttack: Complexity DDoS attack on DNS Recursive Resolvers</b> .....	<b>3187</b>
Yehuda Afek and Anat Bremler-Barr, <i>Tel-Aviv University</i> ; Shani Stajnsrod, <i>Reichman University</i>	
<b>Graphs and Security</b>	
<b>Inductive Graph Unlearning</b> .....	<b>3205</b>
Cheng-Long Wang, <i>King Abdullah University of Science and Technology and SDAIA-KAUST Center of Excellence in Data Science and Artificial Intelligence</i> ; Mengdi Huai, <i>Iowa State University</i> ; Di Wang, <i>King Abdullah University of Science and Technology, Computational Bioscience Research Center, and SDAIA-KAUST Center of Excellence in Data Science and Artificial Intelligence</i>	
<b>GAP: Differentially Private Graph Neural Networks with Aggregation Perturbation</b> .....	<b>3223</b>
Sina Sajadmanesh, <i>Idiap Research Institute and EPFL</i> ; Ali Shahin Shamsabadi, <i>Alan Turing Institute</i> ; Aurélien Bellet, <i>Inria</i> ; Daniel Gatica-Perez, <i>Idiap Research Institute and EPFL</i>	
<b>PrivGraph: Differentially Private Graph Data Publication by Exploiting Community Information</b> .....	<b>3241</b>
Quan Yuan, <i>Zhejiang University</i> ; Zhikun Zhang, <i>Stanford University and CISPA Helmholtz Center for Information Security</i> ; Linkang Du, <i>Zhejiang University</i> ; Min Chen, <i>CISPA Helmholtz Center for Information Security</i> ; Peng Cheng and Mingyang Sun, <i>Zhejiang University</i>	
<b>On the Security Risks of Knowledge Graph Reasoning</b> .....	<b>3259</b>
Zhaohan Xi, Tianyu Du, Changjiang Li, and Ren Pang, <i>Pennsylvania State University</i> ; Shouling Ji, <i>Zhejiang University</i> ; Xiapu Luo, <i>The Hong Kong Polytechnic University</i> ; Xusheng Xiao, <i>Arizona State University</i> ; Fenglong Ma and Ting Wang, <i>Pennsylvania State University</i>	
<b>The Case for Learned Provenance Graph Storage Systems</b> .....	<b>3277</b>
Hailun Ding, Juan Zhai, Dong Deng, and Shiqing Ma, <i>Rutgers University</i>	
<b>Ethereum Security</b>	
<b>A Large Scale Study of the Ethereum Arbitrage Ecosystem</b> .....	<b>3295</b>
Robert McLaughlin, Christopher Kruegel, and Giovanni Vigna, <i>University of California, Santa Barbara</i>	
<b>ACON<sup>2</sup>: Adaptive Conformal Consensus for Provable Blockchain Oracles</b> .....	<b>3313</b>
Sangdon Park, <i>Georgia Institute of Technology</i> ; Osbert Bastani, <i>University of Pennsylvania</i> ; Taesoo Kim, <i>Georgia Institute of Technology</i>	

<b>Snapping Snap Sync: Practical Attacks on Go Ethereum Synchronising Nodes</b> . . . . .	<b>3331</b>
Massimiliano Taverna and Kenneth G. Paterson, <i>ETH Zurich</i>	
<b>Token Spammers, Rug Pulls, and Sniper Bots: An Analysis of the Ecosystem of Tokens in Ethereum and in the Binance Smart Chain (BNB)</b> . . . . .	<b>3349</b>
Federico Cernera, Massimo La Morgia, Alessandro Mei, and Francesco Sassi, <i>Sapienza University of Rome</i>	
<b>Automated Inference on Financial Security of Ethereum Smart Contracts</b> . . . . .	<b>3367</b>
Wansen Wang and Wenchao Huang, <i>University of Science and Technology of China</i> ; Zhaoyi Meng, <i>Anhui University</i> ; Yan Xiong and Fuyou Miao, <i>University of Science and Technology of China</i> ; Xianjin Fang, <i>Anhui University of Science and Technology</i> ; Caichang Tu and Renjie Ji, <i>University of Science and Technology of China</i>	
<b>Supply Chains and Third-Party Code</b>	
<b>LibScan: Towards More Precise Third-Party Library Identification for Android Applications</b> . . . . .	<b>3385</b>
Yafei Wu and Cong Sun, <i>State Key Lab of ISN, School of Cyber Engineering, Xidian University, China</i> ; Dongrui Zeng, <i>Palo Alto Networks, Inc., Santa Clara, CA, USA</i> ; Gang Tan, <i>The Pennsylvania State University, University Park, PA, USA</i> ; Siqi Ma, <i>University of New South Wales, Australia</i> ; Peicheng Wang, <i>State Key Lab of ISN, School of Cyber Engineering, Xidian University, China</i>	
<b>Union under Duress: Understanding Hazards of Duplicate Resource Mismediation in Android Software Supply Chain</b> . . . . .	<b>3403</b>
Xueqiang Wang, <i>University of Central Florida</i> ; Yifan Zhang and XiaoFeng Wang, <i>Indiana University Bloomington</i> ; Yan Jia, <i>Nankai University</i> ; Luyi Xing, <i>Indiana University Bloomington</i>	
<b>UVSCAN: Detecting Third-Party Component Usage Violations in IoT Firmware</b> . . . . .	<b>3421</b>
Binbin Zhao, <i>Georgia Institute of Technology and Zhejiang University</i> ; Shouling Ji and Xuhong Zhang, <i>Zhejiang University</i> ; Yuan Tian, <i>University of California, Los Angeles</i> ; Qinying Wang, Yuwen Pu, and Chenyang Lyu, <i>Zhejiang University</i> ; Raheem Beyah, <i>Georgia Institute of Technology</i>	
<b>Beyond Typosquatting: An In-depth Look at Package Confusion</b> . . . . .	<b>3439</b>
Shradha Neupane, <i>Worcester Polytechnic Institute</i> ; Grant Holmes, Elizabeth Wyss, and Drew Davidson, <i>University of Kansas</i> ; Lorenzo De Carli, <i>University of Calgary</i>	
<b>SANDRILLER: A Fully-Automated Approach for Testing Language-Based JavaScript Sandboxes</b> . . . . .	<b>3457</b>
Abdullah AlHamdan and Cristian-Alexandru Staicu, <i>CISPA Helmholtz Center for Information Security</i>	
<b>Cellular Networks</b>	
<b>Instructions Unclear: Undefined Behaviour in Cellular Network Specifications</b> . . . . .	<b>3475</b>
Daniel Klischies, <i>Ruhr University Bochum</i> ; Moritz Schloegel and Tobias Scharnowski, <i>CISPA Helmholtz Center for Information Security</i> ; Mikhail Bogodukhov, <i>Independent</i> ; David Rupprecht, <i>Radix Security</i> ; Veelasha Moonsamy, <i>Ruhr University Bochum</i>	
<b>MOBILEATLAS: Geographically Decoupled Measurements in Cellular Networks for Security and Privacy Research</b> . .	<b>3493</b>
Gabriel K. Gegenhuber, <i>University of Vienna</i> ; Wilfried Mayer, <i>SBA Research</i> ; Edgar Weippl, <i>University of Vienna</i> ; Adrian Dabrowski, <i>CISPA Helmholtz Center for Information Security</i>	
<b>Eavesdropping Mobile App Activity via Radio-Frequency Energy Harvesting</b> . . . . .	<b>3511</b>
Tao Ni, <i>Shenzhen Research Institute, City University of Hong Kong, and Department of Computer Science, City University of Hong Kong</i> ; Guohao Lan, <i>Department of Software Technology, Delft University of Technology</i> ; Jia Wang, <i>College of Computer Science and Software Engineering, Shenzhen University</i> ; Qingchuan Zhao, <i>Department of Computer Science, City University of Hong Kong</i> ; Weitao Xu, <i>Shenzhen Research Institute, City University of Hong Kong, and Department of Computer Science, City University of Hong Kong</i>	
<b>Sherlock on Specs: Building LTE Conformance Tests through Automated Reasoning</b> . . . . .	<b>3529</b>
Yi Chen and Di Tang, <i>Indiana University Bloomington</i> ; Yepeng Yao, <i>{CAS-KLONAT, BKLONSPT}, Institute of Information Engineering, CAS, and School of Cyber Security, University of Chinese Academy of Sciences</i> ; Mingming Zha and Xiaofeng Wang, <i>Indiana University Bloomington</i> ; Xiaozhong Liu, <i>Worcester Polytechnic Institute</i> ; Haixu Tang, <i>Indiana University Bloomington</i> ; Baoxu Liu, <i>{CAS-KLONAT, BKLONSPT}, Institute of Information Engineering, CAS, and School of Cyber Security, University of Chinese Academy of Sciences</i>	

**BASECOMP: A Comparative Analysis for Integrity Protection in Cellular Baseband Software** ..... 3547  
Eunsoo Kim, Min Woo Baek, and CheolJun Park, *KAIST*; Dongkwan Kim, *Samsung SDS*; Yongdae Kim and Insu Yun, *KAIST*

## Usability and User Perspectives

**Investigating Verification Behavior and Perceptions of Visual Digital Certificates** ..... 3565  
Dañiel Gerhardt and Alexander Ponticello, *CISPA Helmholtz Center for Information Security and Saarland University*;  
Adrian Dabrowski and Katharina Krombholz, *CISPA Helmholtz Center for Information Security*

**“My Privacy for their Security”: Employees’ Privacy Perspectives and Expectations when using Enterprise Security Software** ..... 3583  
Jonah Stegman, Patrick J. Trottier, Caroline Hillier, and Hassan Khan, *University of Guelph*; Mohammad Mannan, *Concordia University*

**Account Security Interfaces: Important, Unintuitive, and Untrustworthy.** ..... 3601  
Alaa Daffalla and Marina Bohuk, *Cornell University*; Nicola Dell, *Jacobs Institute Cornell Tech*; Rosanna Bellini, *Cornell University*; Thomas Ristenpart, *Cornell Tech*

**Defining “Broken”: User Experiences and Remediation Tactics When Ad-Blocking or Tracking-Protection Tools Break a Website’s User Experience** ..... 3619  
Alexandra Nisenoff, *University of Chicago and Carnegie Mellon University*; Arthur Borem, Madison Pickering, Grant Nakanishi, Maya Thumpasery, and Blase Ur, *University of Chicago*

**Cryptographic Deniability: A Multi-perspective Study of User Perceptions and Expectations.** ..... 3637  
Tarun Kumar Yadav, *Brigham Young University*; Devashish Gosain, *KU Leuven*; Kent Seamons, *Brigham Young University*

## Entomology

**Silent Bugs Matter: A Study of Compiler-Introduced Security Bugs** ..... 3655  
Jianhao Xu, *Nanjing University*; Kangjie Lu, *University of Minnesota*; Zhengjie Du, Zhu Ding, and Linke Li, *Nanjing University*; Qiushi Wu, *University of Minnesota*; Mathias Payer, *EPFL*; Bing Mao, *Nanjing University*

**A Bug’s Life: Analyzing the Lifecycle and Mitigation Process of Content Security Policy Bugs** ..... 3673  
Gertjan Franken, Tom Van Goethem, Lieven Desmet, and Wouter Joosen, *imec-DistriNet, KU Leuven*

**Remote Code Execution from SSTI in the Sandbox: Automatically Detecting and Exploiting Template Escape Bugs** ..... 3691  
Yudi Zhao, Yuan Zhang, and Min Yang, *Fudan University*

**Detecting API Post-Handling Bugs Using Code and Description in Patches** ..... 3709  
Miaoqian Lin, Kai Chen, and Yang Xiao, *Institute of Information Engineering, Chinese Academy of Sciences, China*; *School of Cyber Security, University of Chinese Academy of Sciences, China*

**Place Your Locks Well: Understanding and Detecting Lock Misuse Bugs.** ..... 3727  
Yuandao Cai, Peisen Yao, Chengfeng Ye, and Charles Zhang, *The Hong Kong University of Science and Technology*

## Adversarial Examples

**The Space of Adversarial Strategies** ..... 3745  
Ryan Sheatsley, Blaine Hoak, Eric Pauley, and Patrick McDaniel, *University of Wisconsin-Madison*

**“Security is not my field, I’m a stats guy”: A Qualitative Root Cause Analysis of Barriers to Adversarial Machine Learning Defenses in Industry** ..... 3763  
Jaron Mink, *University of Illinois at Urbana-Champaign*; Harjot Kaur, *Leibniz University Hannover*; Juliane Schmußer and Sascha Fahl, *CISPA Helmholtz Center for Information Security*; Yasemin Acar, *Paderborn University and George Washington University*

**X-Adv: Physical Adversarial Object Attacks against X-ray Prohibited Item Detection** ..... 3781  
Aishan Liu and Jun Guo, *Beihang University*; Jiakai Wang, *Zhongguancun Laboratory*; Siyuan Liang, *Chinese Academy of Sciences*; Renshuai Tao, *Beihang University*; Wenbo Zhou, *University of Science and Technology of China*; Cong Liu, *iFLYTEK*; Xianglong Liu, *Beihang University, Zhongguancun Laboratory, and Hefei Comprehensive National Science Center*; Dacheng Tao, *JD Explore Academy*



<b>SMACK: Semantically Meaningful Adversarial Audio Attack</b> . . . . .	<b>3799</b>
Zhiyuan Yu, Yuanhaur Chang, and Ning Zhang, <i>Washington University in St. Louis</i> ; Chaowei Xiao, <i>Arizona State University</i>	
<b>URET: Universal Robustness Evaluation Toolkit (for Evasion)</b> . . . . .	<b>3817</b>
Kevin Eykholt, Taesung Lee, Douglas Schales, Jiyong Jang, and Ian Molloy, <i>IBM Research</i> ; Masha Zorin, <i>University of Cambridge</i>	
<b>Private Record Access</b>	
<b>Authenticated private information retrieval</b> . . . . .	<b>3835</b>
Simone Colombo, <i>EPFL</i> ; Kirill Nikitin, <i>Cornell Tech</i> ; Henry Corrigan-Gibbs, <i>MIT</i> ; David J. Wu, <i>UT Austin</i> ; Bryan Ford, <i>EPFL</i>	
<b>Don't be Dense: Efficient Keyword PIR for Sparse Databases</b> . . . . .	<b>3853</b>
Sarvar Patel and Joon Young Seo, <i>Google</i> ; Kevin Yeo, <i>Google and Columbia University</i>	
<b>GigaDORAM: Breaking the Billion Address Barrier</b> . . . . .	<b>3871</b>
Brett Falk, <i>University of Pennsylvania</i> ; Rafail Ostrovsky, Matan Shtepel, and Jacob Zhang, <i>University of California, Los Angeles</i>	
<b>One Server for the Price of Two: Simple and Fast Single-Server Private Information Retrieval</b> . . . . .	<b>3889</b>
Alexandra Henzinger, Matthew M. Hong, and Henry Corrigan-Gibbs, <i>MIT</i> ; Sarah Meiklejohn, <i>Google</i> ; Vinod Vaikuntanathan, <i>MIT</i>	
<b>DUORAM: A Bandwidth-Efficient Distributed ORAM for 2- and 3-Party Computation</b> . . . . .	<b>3907</b>
Adithya Vadapalli, <i>University of Waterloo</i> ; Ryan Henry, <i>University of Calgary</i> ; Ian Goldberg, <i>University of Waterloo</i>	
<b>It's All Fun and Games Until...</b>	
<b>A Peek into the Metaverse: Detecting 3D Model Clones in Mobile Games</b> . . . . .	<b>3925</b>
Chaoshun Zuo, Chao Wang, and Zhiqiang Lin, <i>The Ohio State University</i>	
<b>PATROL: Provable Defense against Adversarial Policy in Two-player Games</b> . . . . .	<b>3943</b>
Wenbo Guo, <i>UC Berkeley</i> ; Xian Wu, <i>Northwestern University</i> ; Lun Wang, <i>UC Berkeley</i> ; Xinyu Xing, <i>Northwestern University</i> ; Dawn Song, <i>UC Berkeley</i>	
<b>The Blockchain Imitation Game</b> . . . . .	<b>3961</b>
Kaihua Qin, <i>Imperial College London, RDI</i> ; Stefanos Chaliasos, <i>Imperial College London</i> ; Liyi Zhou, <i>Imperial College London, RDI</i> ; Benjamin Livshits, <i>Imperial College London</i> ; Dawn Song, <i>UC Berkeley, RDI</i> ; Arthur Gervais, <i>University College London, RDI</i>	
<b>It's all in your head(set): Side-channel attacks on AR/VR systems</b> . . . . .	<b>3979</b>
Yicheng Zhang, Carter Slocum, Jiasi Chen, and Nael Abu-Ghazaleh, <i>University of California, Riverside</i>	
<b>Egg Hunt in Tesla Infotainment: A First Look at Reverse Engineering of Qt Binaries</b> . . . . .	<b>3997</b>
Haohuang Wen and Zhiqiang Lin, <i>The Ohio State University</i>	
<b>Enclaves and Serverless Computing</b>	
<b>Reusable Enclaves for Confidential Serverless Computing</b> . . . . .	<b>4015</b>
Shixuan Zhao, <i>The Ohio State University</i> ; Pinshen Xu, <i>Southern University of Science and Technology</i> ; Guoxing Chen, <i>Shanghai Jiao Tong University</i> ; Mengya Zhang, <i>The Ohio State University</i> ; Yinqian Zhang, <i>Southern University of Science and Technology</i> ; Zhiqiang Lin, <i>The Ohio State University</i>	
<b>ENIGMAP: External-Memory Oblivious Map for Secure Enclaves</b> . . . . .	<b>4033</b>
Afonso Tinoco, Sixiang Gao, and Elaine Shi, <i>CMU</i>	
<b>AEX-Notify: Thwarting Precise Single-Stepping Attacks through Interrupt Awareness for Intel SGX Enclaves</b> . . . . .	<b>4051</b>
Scott Constable, <i>Intel Corporation</i> ; Jo Van Bulck, <i>imec-DistriNet, KU Leuven</i> ; Xiang Cheng, <i>Georgia Institute of Technology</i> ; Yuan Xiao, Cedric Xing, and Ilya Alexandrovich, <i>Intel Corporation</i> ; Taesoo Kim, <i>Georgia Institute of Technology</i> ; Frank Piessens, <i>imec-DistriNet, KU Leuven</i> ; Mona Vij, <i>Intel Corporation</i> ; Mark Silberstein, <i>Technion</i>	
<b>Controlled Data Races in Enclaves: Attacks and Detection</b> . . . . .	<b>4069</b>
Sanchuan Chen, <i>Fordham University</i> ; Zhiqiang Lin, <i>The Ohio State University</i> ; Yinqian Zhang, <i>Southern University of Science and Technology</i>	

**Guarding Serverless Applications with Kalium** ..... 4087  
Deepak Sirone Jegan, *University of Wisconsin-Madison*; Liang Wang, *Princeton University*; Siddhant Bhagat, *Microsoft*;  
Michael Swift, *University of Wisconsin-Madison*

## **Email and Phishing**

**“To Do This Properly, You Need More Resources”: The Hidden Costs of Introducing Simulated Phishing Campaigns**..... 4105  
Lina Brunken, Annalina Buckmann, Jonas Hielscher, and M. Angela Sasse, *Ruhr University Bochum*

**You’ve Got Report: Measurement and Security Implications of DMARC Reporting** ..... 4123  
Md. Ishtiaq Ashiq and Weitong Li, *Virginia Tech*; Tobias Fiebig, *Max-Planck-Institut für Informatik*; Taejoong Chung, *Virginia Tech*

**Knowledge Expansion and Counterfactual Interaction for Reference-Based Phishing Detection**..... 4139  
Ruofan Liu, *Shanghai Jiao Tong University and National University of Singapore*; Yun Lin, *Shanghai Jiao Tong University*;  
Yifan Zhang, Penn Han Lee, and Jin Song Dong, *National University of Singapore*

**Rods with Laser Beams: Understanding Browser Fingerprinting on Phishing Pages** ..... 4157  
Iskander Sanchez-Rola and Leyla Bilge, *Norton Research Group*; Davide Balzarotti, *EURECOM*; Armin Buescher, *Crosspoint Labs*; Petros Efstathopoulos, *Norton Research Group*

**Content-Type: multipart/oracle - Tapping into Format Oracles in Email End-to-End Encryption** ..... 4175  
Fabian Insing, *Münster University of Applied Sciences and National Research Center for Applied Cybersecurity ATHENE*;  
Damian Poddebniak and Tobias Kappert, *Münster University of Applied Sciences*; Christoph Saatjohann and Sebastian Schinzel, *Münster University of Applied Sciences and National Research Center for Applied Cybersecurity ATHENE*

## **OSes and Security**

**PET: Prevent Discovered Errors from Being Triggered in the Linux Kernel** ..... 4193  
Zicheng Wang, *Nanjing University*; Yueqi Chen, *University of Colorado Boulder*; Qingkai Zeng, *Nanjing University*

**A Hybrid Alias Analysis and Its Application to Global Variable Protection in the Linux Kernel** ..... 4211  
Guoren Li, *University of California, Riverside*; Hang Zhang, *Georgia Institute of Technology*; Jinmeng Zhou and Wenbo Shen, *Zhejiang University*; Yulei Sui, *University of New South Wales*; Zhiyun Qian, *University of California, Riverside*

**AlphaEXP: An Expert System for Identifying Security-Sensitive Kernel Objects** ..... 4229  
Ruipeng Wang, *National University of Defense Technology*; Kaixiang Chen and Chao Zhang, *Tsinghua University*;  
Zulie Pan and Qianyu Li, *National University of Defense Technology*; Siliang Qin, *University of Chinese Academy of Sciences*; Shenglin Xu, Min Zhang, and Yang Li, *National University of Defense Technology*

**Mitigating Security Risks in Linux with KLAUS: A Method for Evaluating Patch Correctness** ..... 4247  
Yuhang Wu and Zhenpeng Lin, *Northwestern University*; Yueqi Chen, *University of Colorado Boulder*; Dang K Le, *Northwestern University*; Dongliang Mu, *Huazhong University of Science and Technology*; Xinyu Xing, *Northwestern University*

**Detecting Union Type Confusion in Component Object Model**..... 4265  
Yuxing Zhang, *East China Normal University*; Xiaogang Zhu, *Swinburne University of Technology*; Daojing He, *East China Normal University*; Harbin Institute of Technology, *Shenzhen*; Minhui Xue, *CSIRO’s Data61*; Shouling Ji, *Zhejiang University*; Mohammad Sayad Haghighi and Sheng Wen, *Swinburne University of Technology*; Zhiniang Peng, *Sangfor Technologies Inc.*

## **Intrusion Detection**

**Network Detection of Interactive SSH Impostors Using Deep Learning** ..... 4283  
Julien Piet, *UC Berkeley and Corelight*; Aashish Sharma, *Lawrence Berkeley National Laboratory*; Vern Paxson, *Corelight and UC Berkeley*; David Wagner, *UC Berkeley*

**ARGUS: Context-Based Detection of Stealthy IoT Infiltration Attacks**..... 4301  
Phillip Rieger, Marco Chilese, Reham Mohamed, Markus Miettinen, Hossein Fereidooni, and Ahmad-Reza Sadeghi, *Technical University of Darmstadt*

<b>Generative Intrusion Detection and Prevention on Data Stream</b> .....	<b>4319</b>
HyungBin Seo and MyungKeun Yoon, <i>Kookmin University</i>	
<b>xNIDS: Explaining Deep Learning-based Network Intrusion Detection Systems for Active Intrusion Responses</b> ..	<b>4337</b>
Feng Wei, <i>University at Buffalo</i> ; Hongda Li, <i>Palo Alto Networks</i> ; Ziming Zhao and Hongxin Hu, <i>University at Buffalo</i>	
<b>PROGRAPHER: An Anomaly Detection System based on Provenance Graph Embedding</b> .....	<b>4355</b>
Fan Yang, <i>The Chinese University of Hong Kong</i> ; Jiacen Xu, <i>University of California, Irvine</i> ; Chunlin Xiong, <i>Sangfor Technologies Inc.</i> ; Zhou Li, <i>University of California, Irvine</i> ; Kehuan Zhang, <i>The Chinese University of Hong Kong</i>	
<b>Privacy Preserving Crypto Blocks</b>	
<b>Dubhe: Succinct Zero-Knowledge Proofs for Standard AES and related Applications</b> .....	<b>4373</b>
Changchang Ding and Yan Huang, <i>Indiana University Bloomington</i>	
<b>Curve Trees: Practical and Transparent Zero-Knowledge Accumulators</b> .....	<b>4391</b>
Matteo Campanelli, <i>Protocol Labs</i> ; Mathias Hall-Andersen and Simon Holmgard Kamp, <i>Aarhus University, Denmark</i>	
<b>BalanceProofs: Maintainable Vector Commitments with Fast Aggregation</b> .....	<b>4409</b>
Weijie Wang, Annie Ulichney, and Charalampos Papamanthou, <i>Yale University</i>	
<b>zkSaaS: Zero-Knowledge SNARKs as a Service</b> .....	<b>4427</b>
Sanjam Garg, <i>University of California, Berkeley, and NTT Research</i> ; Aarushi Goel, <i>NTT Research</i> ; Abhishek Jain, <i>Johns Hopkins University</i> ; Guru-Vamsi Policharla and Sruthi Sekar, <i>University of California, Berkeley</i>	
<b>VERIZEXE: Decentralized Private Computation with Universal Setup</b> .....	<b>4445</b>
Alex Luoyuan Xiong, <i>Espresso Systems, National University of Singapore</i> ; Binyi Chen and Zhenfei Zhang, <i>Espresso Systems</i> ; Benedikt Bünz, <i>Espresso Systems, Stanford University</i> ; Ben Fisch, <i>Espresso Systems, Yale University</i> ; Fernando Krell and Philippe Camacho, <i>Espresso Systems</i>	
<b>Warm and Fuzzing</b>	
<b>INTENDER: Fuzzing Intent-Based Networking with Intent-State Transition Guidance</b> .....	<b>4463</b>
Jiwon Kim, <i>Purdue University</i> ; Benjamin E. Ujcich, <i>Georgetown University</i> ; Dave (Jing) Tian, <i>Purdue University</i>	
<b>BLEEM: Packet Sequence Oriented Fuzzing for Protocol Implementations</b> .....	<b>4481</b>
Zhengxiong Luo, Junze Yu, Feilong Zuo, Jianzhong Liu, and Yu Jiang, <i>Tsinghua University</i> ; Ting Chen, <i>University of Electronic Science and Technology of China</i> ; Abhik Roychoudhury, <i>National University of Singapore</i> ; Jianguang Sun, <i>Tsinghua University</i>	
<b>Automated Exploitable Heap Layout Generation for Heap Overflows Through Manipulation</b>	
<b>Distance-Guided Fuzzing</b> .....	<b>4499</b>
Bin Zhang, Jiongyi Chen, Runhao Li, Chao Feng, Ruilin Li, and Chaojing Tang, <i>National University of Defense Technology</i>	
<b>MINER: A Hybrid Data-Driven Approach for REST API Fuzzing</b> .....	<b>4517</b>
Chenyang Lyu, Jiacheng Xu, Shouling Ji, Xuhong Zhang, and Qinying Wang, <i>Zhejiang University</i> ; Binbin Zhao, <i>Georgia Institute of Technology</i> ; Gaoning Pan, <i>Zhejiang University</i> ; Wei Cao and Peng Chen, <i>Ant Group</i> ; Raheem Beyah, <i>Georgia Institute of Technology</i>	
<b>Systematic Assessment of Fuzzers using Mutation Analysis</b> .....	<b>4535</b>
Philipp Görz, Björn Mathis, and Keno Hassler, <i>CISPA Helmholtz Center for Information Security</i> ; Emre Güler, <i>Ruhr-Universität Bochum</i> ; Thorsten Holz and Andreas Zeller, <i>CISPA Helmholtz Center for Information Security</i> ; Rahul Gopinath, <i>University of Sydney</i>	
<b>Remote Attacks</b>	
<b>HOME SPY: The Invisible Sniffer of Infrared Remote Control of Smart TVs</b> .....	<b>4553</b>
Kong Huang, YuTong Zhou, and Ke Zhang, <i>The Chinese University of Hong Kong</i> ; Jiacen Xu, <i>University of California, Irvine</i> ; Jiongyi Chen, <i>National University of Defense Technology</i> ; Di Tang, <i>Indiana University Bloomington</i> ; Kehuan Zhang, <i>The Chinese University of Hong Kong</i>	

**Remote Attacks on Speech Recognition Systems Using Sound from Power Supply** ..... 4571  
Lanqing Yang, Xinqi Chen, Xiangyong Jian, Leping Yang, Yijie Li, Qianfei Ren, Yi-Chao Chen, and Guangtao Xue,  
*Shanghai Jiao Tong University; Xiaoyu Ji, Zhejiang University*

**Near-Ultrasound Inaudible Trojan (NUIT): Exploiting Your Speaker to Attack Your Microphone** ..... 4589  
Qi Xia and Qian Chen, *University of Texas at San Antonio; Shouhuai Xu, University of Colorado Colorado Springs*

**Medusa Attack: Exploring Security Hazards of In-App QR Code Scanning** ..... 4607  
Xing Han, Yuheng Zhang, and Xue Zhang, *University of Electronic Science and Technology of China and Shanghai Qi Zhi Institute; Zeyuan Chen, G.O.S.S.I.P; Mingzhe Wang, Xidian University; Yiwei Zhang, Purdue University; Siqi Ma, The University of New South Wales; Yu Yu, Shanghai Qi Zhi Institute and Shanghai Jiao Tong University; Elisa Bertino, Purdue University; Juanru Li, Shanghai Qi Zhi Institute and Shanghai Jiao Tong University*

## **Understanding Communities, Part 1**

**Othered, Silenced and Scapegoated: Understanding the Situated Security of Marginalised Populations in Lebanon** ..... 4625  
Jessica McClearn and Rikke Bjerg Jensen, *Royal Holloway, University of London; Reem Talhouk, Northumbria University*

**Examining Power Dynamics and User Privacy in Smart Technology Use Among Jordanian Households** ..... 4643  
Wael Albayaydh and Ivan Flechais, *University of Oxford*

**“If sighted people know, I should be able to know:” Privacy Perceptions of Bystanders with Visual Impairments around Camera-based Technology** ..... 4661  
Yuhang Zhao, *University of Wisconsin—Madison; Yaxing Yao, University of Maryland, Baltimore County; Jiaru Fu and Nihan Zhou, University of Wisconsin—Madison*

**A Research Framework and Initial Study of Browser Security for the Visually Impaired** ..... 4679  
Elaine Lau and Zachary Peterson, *Cal Poly, San Luis Obispo*

## **Keeping Computations Confidential**

**ELASM: Error-Latency-Aware Scale Management for Fully Homomorphic Encryption** ..... 4697  
Yongwoo Lee, Seonyoung Cheon, and Dongkwan Kim, *Yonsei University; Dongyoon Lee, Stony Brook University; Hanjun Kim, Yonsei University*

**HECO: Fully Homomorphic Encryption Compiler** ..... 4715  
Alexander Viand, Patrick Jattke, Miro Haller, and Anwar Hithnawi, *ETH Zurich*

**A Verified Confidential Computing as a Service Framework for Privacy Preservation** ..... 4733  
Hongbo Chen and Haobin Hiroki Chen, *Indiana University Bloomington; Mingshen Sun, Independent Researcher; Kang Li and Zhaofeng Chen, CertiK; XiaoFeng Wang, Indiana University Bloomington*

**CSHER: A System for Compact Storage with HE-Retrieval** ..... 4751  
Adi Akavia and Neta Oren, *University of Haifa; Boaz Sapir and Margarita Vald, Intuit Israel Inc.*

## **Towards Robust Learning**

**Precise and Generalized Robustness Certification for Neural Networks** ..... 4769  
Yuanyuan Yuan, *The Hong Kong University of Science and Technology and ETH Zurich; Shuai Wang, The Hong Kong University of Science and Technology; Zhendong Su, ETH Zurich*

**DiffSmooth: Certifiably Robust Learning via Diffusion Models and Local Smoothing** ..... 4787  
Jiawei Zhang, *UIUC; Zhongzhu Chen, University of Michigan, Ann Arbor; Huan Zhang, Carnegie Mellon University; Chaowei Xiao, Arizona State University; Bo Li, UIUC*

**ACORN: Input Validation for Secure Aggregation** ..... 4805  
James Bell and Adrià Gascón, *Google LLC; Tancredè Lepoint, Amazon; Baiyu Li, Sarah Meiklejohn, and Mariana Raykova, Google LLC; Cathie Yun*

**HOLMES: Efficient Distribution Testing for Secure Collaborative Learning** ..... 4823  
Ian Chang and Katerina Sotiraki, *UC Berkeley; Weikeng Chen, UC Berkeley & DZK Labs; Murat Kantarcioglu, University of Texas at Dallas & UC Berkeley; Raluca Popa, UC Berkeley*

## Network Cryptographic Protocols

**Keep Your Friends Close, but Your Routers Closer: Insights into RPKI Validation in the Internet . . . . . 4841**

Tomas Hlavacek, *Fraunhofer Institute for Secure Information Technology SIT and National Research Center for Applied Cybersecurity ATHENE*; Haya Shulman and Niklas Vogel, *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*

**Exploring the Unknown DTLS Universe: Analysis of the DTLS Server Ecosystem on the Internet . . . . . 4859**

Nurullah Erinola and Marcel Maehren, *Ruhr University Bochum*; Robert Merget, *Technology Innovation Institute*; Juraj Somorovsky, *Paderborn University*; Jörg Schwenk, *Ruhr University Bochum*

**We Really Need to Talk About Session Tickets: A Large-Scale Analysis of Cryptographic Dangers with TLS Session Tickets . . . . . 4877**

Sven Hebrok, *Paderborn University*; Simon Nachtigall, *Paderborn University and achelos GmbH*; Marcel Maehren and Nurullah Erinola, *Ruhr University Bochum*; Robert Merget, *Technology Innovation Institute and Ruhr University Bochum*; Juraj Somorovsky, *Paderborn University*; Jörg Schwenk, *Ruhr University Bochum*

**Extended Hell(o): A Comprehensive Large-Scale Study on Email Confidentiality and Integrity Mechanisms in the Wild . . . . . 4895**

Birk Blechschmidt, *Saarland University*; Ben Stock, *CISPA Helmholtz Center for Information Security*

## Warmer and Fuzzers

**No Linux, No Problem: Fast and Correct Windows Binary Fuzzing via Target-embedded Snapshotting . . . . . 4913**

Leo Stone and Rishi Ranjan, *Virginia Tech*; Stefan Nagy, *University of Utah*; Matthew Hicks, *Virginia Tech*

**DAFL: Directed Grey-box Fuzzing guided by Data Dependency . . . . . 4931**

Tae Eun Kim, *KAIST*; Jaeseung Choi, *Sogang University*; Kihong Heo and Sang Kil Cha, *KAIST*

**DynSQL: Stateful Fuzzing for Database Management Systems with Complex and Valid SQL Query Generation . . 4949**

Zu-Ming Jiang, *ETH Zurich*; Jia-Ju Bai, *Tsinghua University*; Zhendong Su, *ETH Zurich*

**AIFORE: Smart Fuzzing Based on Automatic Input Format Reverse Engineering . . . . . 4967**

Ji Shi, {*CAS-KLONAT, BKLONSPT*}, *Institute of Information Engineering, Chinese Academy of Sciences; Institute for Network Science and Cyberspace & BNRist, Tsinghua University; Zhongguancun Lab; Singular Security Lab, Huawei Technologies; School of Cyber Security, University of Chinese Academy of Sciences*; Zhun Wang, *Institute for Network Science and Cyberspace & BNRist, Tsinghua University; Zhongguancun Lab*; Zhiyao Feng, *Institute for Network Science and Cyberspace & BNRist, Tsinghua University; Zhongguancun Lab*; EPFL; Yang Lan and Shisong Qin, *Institute for Network Science and Cyberspace & BNRist, Tsinghua University; Zhongguancun Lab*; Wei You, *Renmin University of China*; Wei Zou, {*CAS-KLONAT, BKLONSPT*}, *Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences*; Mathias Payer, *EPFL*; Chao Zhang, *Institute for Network Science and Cyberspace & BNRist, Tsinghua University; Zhongguancun Lab*

## Friday, August 11

### Kernel Analysis

**BoKASAN: Binary-only Kernel Address Sanitizer for Effective Kernel Fuzzing . . . . . 4985**

Mingi Cho, Dohyeon An, Hoyong Jin, and Taekyoung Kwon, *Yonsei University*

**ACTOR: Action-Guided Kernel Fuzzing . . . . . 5003**

Marius Fleischer, Dipanjan Das, and Priyanka Bose, *University of California, Santa Barbara*; Weiheng Bai and Kangjie Lu, *University of Minnesota*; Mathias Payer, *EPFL*; Christopher Kruegel and Giovanni Vigna, *University of California, Santa Barbara*

**FirmSolo: Enabling dynamic analysis of binary Linux-based IoT kernel modules . . . . . 5021**

Ioannis Angelakopoulos, Gianluca Stringhini, and Manuel Egele, *Boston University*

**XextFuzz: Fuzzing macOS Kernel EXTensions on Apple Silicon via Exploiting Mitigations . . . . . 5039**

Tingting Yin, *Tsinghua University and Ant Group*; Zicong Gao, *State Key Laboratory of Mathematical Engineering and Advanced Computing*; Zhenghang Xiao, *Hunan University*; Zheyu Ma, *Tsinghua University*; Min Zheng, *Ant Group*; Chao Zhang, *Tsinghua University and Zhongguancun Laboratory*

**UNCONTAINED: Uncovering Container Confusion in the Linux Kernel**..... 5055  
Jakob Koschel, *Vrije Universiteit Amsterdam*; Pietro Borrello and Daniele Cono D’Elia, *Sapienza University of Rome*;  
Herbert Bos and Cristiano Giuffrida, *Vrije Universiteit Amsterdam*

## **It’s Academic**

**“I’m going to trust this until it burns me” Parents’ Privacy Concerns and Delegation of Trust in K-8 Educational Technology** ..... 5073  
Victoria Zhong, *New York University*; Susan McGregor, *Columbia University*; Rachel Greenstadt, *New York University*

**Educators’ Perspectives of Using (or Not Using) Online Exam Proctoring** ..... 5091  
David G. Balash, Elena Korkes, Miles Grant, and Adam J. Aviv, *The George Washington University*; Rahel A. Fainchtein and Micah Sherr, *Georgetown University*

**No more Reviewer #2: Subverting Automatic Paper-Reviewer Assignment using Adversarial Learning** ..... 5109  
Thorsten Eisenhofer, *Ruhr University Bochum*; Erwin Quiring, *Ruhr University Bochum and International Computer Science Institute (ISCI) Berkeley*; Jonas Möller, *Technische Universität Berlin*; Doreen Riepel, *Ruhr University Bochum*; Thorsten Holz, *CISPA Helmholtz Center for Information Security*; Konrad Rieck, *Technische Universität Berlin*

**A Two-Decade Retrospective Analysis of a University’s Vulnerability to Attacks Exploiting Reused Passwords** .. 5127  
Alexandra Nisenoff, *University of Chicago / Carnegie Mellon University*; Maximilian Golla, *University of Chicago / Max Planck Institute for Security and Privacy*; Miranda Wei, *University of Chicago / University of Washington*; Juliette Hainline, Hayley Szymanek, Annika Braun, Annika Hildebrandt, Blair Christensen, David Langenberg, and Blase Ur, *University of Chicago*

**Ethical Frameworks and Computer Security Trolley Problems: Foundations for Conversations** ..... 5145  
Tadayoshi Kohno, *University of Washington*; Yasemin Acar, *Paderborn University & George Washington University*; Wulf Loh, *Universität Tübingen*

## **De-anonymization and Re-identification**

**CATCH YOU AND I CAN: Revealing Source Voiceprint Against Voice Conversion**..... 5163  
Jiangyi Deng, Yanjiao Chen, Yinan Zhong, and Qianhao Miao, *Zhejiang University*; Xueluan Gong, *Wuhan University*; Wenyan Xu, *Zhejiang University*

**V-CLOAK: Intelligibility-, Naturalness- & Timbre-Preserving Real-Time Voice Anonymization** ..... 5181  
Jiangyi Deng, Fei Teng, and Yanjiao Chen, *Zhejiang University*; Xiaofu Chen and Zhaohui Wang, *Wuhan University*; Wenyan Xu, *Zhejiang University*

**Assessing Anonymity Techniques Employed in German Court Decisions: A De-Anonymization Experiment** .... 5199  
Dominic Deuber and Michael Keuchen, *Friedrich-Alexander-Universität Erlangen-Nürnberg*; Nicolas Christin, *Carnegie Mellon University*

**Person Re-identification in 3D Space: A WiFi Vision-based Approach** ..... 5217  
Yili Ren and Yichao Wang, *Florida State University*; Sheng Tan, *Trinity University*; Yingying Chen, *Rutgers University*; Jie Yang, *Florida State University*

**In the Quest to Protect Users from Side-Channel Attacks – A User-Centred Design Space to Mitigate Thermal Attacks on Public Payment Terminals** ..... 5235  
Karola Marky, *Ruhr-University Bochum and University of Glasgow*; Shaun Macdonald, *University of Glasgow*; Yasmeen Abdrabou, *Lancaster University*; Mohamed Khamis, *University of Glasgow*

## **Thieves in the House**

**Extracting Training Data from Diffusion Models**..... 5253  
Nicholas Carlini, *Google*; Jamie Hayes, *DeepMind*; Milad Nasr and Matthew Jagielski, *Google*; Vikash Sehwal, *Princeton University*; Florian Tramèr, *ETH Zurich*; Borja Balle, *DeepMind*; Daphne Ippolito, *Google*; Eric Wallace, *UC Berkeley*

**PCAT: Functionality and Data Stealing from Split Learning by Pseudo-Client Attack**..... 5271  
Xinben Gao and Lan Zhang, *University of Science and Technology of China*

**A Plot is Worth a Thousand Words: Model Information Stealing Attacks via Scientific Plots** . . . . . 5289  
Boyang Zhang and Xinlei He, *CISPA Helmholtz Center for Information Security*; Yun Shen, *NetApp*; Tianhao Wang, *University of Virginia*; Yang Zhang, *CISPA Helmholtz Center for Information Security*

**Beyond The Gates: An Empirical Analysis of HTTP-Managed Password Stealers and Operators** . . . . . 5307  
Athanasios Avgetidis, Omar Alrawi, Kevin Valakuzhy, and Charles Lever, *Georgia Institute of Technology*; Paul Burbage, *MalBeacon*; Angelos D. Keromytis, Fabian Monrose, and Manos Antonakakis, *Georgia Institute of Technology*

**LightThief: Your Optical Communication Information is Stolen behind the Wall** . . . . . 5325  
Xin Liu, *The Ohio State University*; Wei Wang, *Saint Louis University*; Guanqun Song and Ting Zhu, *The Ohio State University*

## Distributed Secure Computations

**WaterBear: Practical Asynchronous BFT Matching Security Guarantees of Partially Synchronous BFT** . . . . . 5341  
Haibin Zhang, *Beijing Institute of Technology*; Sisi Duan, *Tsinghua University, Zhongguancun Laboratory*; Boxin Zhao, *Zhongguancun Laboratory*; Liehuang Zhu, *Beijing Institute of Technology*

**Practical Asynchronous High-threshold Distributed Key Generation and Distributed Polynomial Sampling** . . . . . 5359  
Sourav Das, *University of Illinois at Urbana-Champaign*; Zhuolun Xiang, *Aptos*; Lefteris Kokoris-Kogias, *IST Austria and Mysten Labs*; Ling Ren, *University of Illinois at Urbana-Champaign*

**Efficient 3PC for Binary Circuits with Application to Maliciously-Secure DNN Inference** . . . . . 5377  
Yun Li, *Tsinghua University, Ant Group*; Yufei Duan, *Tsinghua University*; Zhicong Huang, *Alibaba Group*; Cheng Hong, *Ant Group*; Chao Zhang and Yifan Song, *Tsinghua University*

**TVA: A multi-party computation system for secure and expressive time series analytics** . . . . . 5395  
Muhammad Faisal, *Boston University*; Jerry Zhang, *University of California San Diego*; John Liagouris, *Vasiliki Kalavri*, and Mayank Varia, *Boston University*

**Long Live The Honey Badger: Robust Asynchronous DPSS and its Applications** . . . . . 5413  
Thomas Yurek, *University of Illinois at Urbana-Champaign, NTT Research, and IC3*; Zhuolun Xiang, *Aptos*; Yu Xia, *MIT CSAIL and NTT Research*; Andrew Miller, *University of Illinois at Urbana-Champaign and IC3*

## Mobile Security and Privacy

**Powering Privacy: On the Energy Demand and Feasibility of Anonymity Networks on Smartphones** . . . . . 5431  
Daniel Hugenroth and Alastair R. Beresford, *University of Cambridge*

**EYE-SHIELD: Real-Time Protection of Mobile Device Screen Information from Shoulder Surfing** . . . . . 5449  
Brian Jay Tang and Kang G. Shin, *University of Michigan*

**The OK Is Not Enough: A Large Scale Study of Consent Dialogs in Smartphone Applications** . . . . . 5467  
Simon Koch, *TU Braunschweig*; Benjamin Altpeter, *Datenanfragen.de e.V.*; Martin Johns, *TU Braunschweig*

**Notice the Imposter! A Study on User Tag Spoofing Attack in Mobile Apps** . . . . . 5485  
Shuai Li, Zhemin Yang, Guangliang Yang, Hange Zhang, Nan Hua, Yurui Huang, and Min Yang, *Fudan University*

**Lost in Conversion: Exploit Data Structure Conversion with Attribute Loss to Break Android Systems** . . . . . 5503  
Rui Li, *School of Cyber Science and Technology, Shandong University; Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, SDU; The Chinese University of Hong Kong*; Wenrui Diao and Shishuai Yang, *School of Cyber Science and Technology, Shandong University; Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, SDU*; Xiangyu Liu, *Alibaba Group*; Shanqing Guo, *School of Cyber Science and Technology, Shandong University; Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, SDU*; Kehuan Zhang, *The Chinese University of Hong Kong*

## Web Security

**Silent Spring: Prototype Pollution Leads to Remote Code Execution in Node.js** . . . . . 5521  
Mikhail Shcherbakov and Musard Balliu, *KTH Royal Institute of Technology*; Cristian-Alexandru Staicu, *CISPA Helmholtz Center for Information Security*

**Cookie Crumbles: Breaking and Fixing Web Session Integrity** . . . . . 5539  
Marco Squarcina, *TU Wien*; Pedro Adão, *Instituto Superior Técnico, ULisboa, Instituto de Telecomunicações*; Lorenzo Veronese and Matteo Maffei, *TU Wien*

**Minimalist: Semi-automated Debloating of PHP Web Applications through Static Analysis** ..... 5577  
Rasoul Jahanshahi, *Boston University*; Babak Amin Azad and Nick Nikiforakis, *Stony Brook University*; Manuel Egele, *Boston University*

**AnimateDead: Debloating Web Applications Using Concolic Execution** ..... 5575  
Babak Amin Azad, *Stony Brook University*; Rasoul Jahanshahi, *Boston University*; Chris Tsoukaladelis, *Stony Brook University*; Manuel Egele, *Boston University*; Nick Nikiforakis, *Stony Brook University*

**NAUTILUS: Automated RESTful API Vulnerability Detection.** ..... 5593  
Gelei Deng, *Nanyang Technological University*; Zhiyi Zhang, *CodeSafe Team, Qi An Xin Group Corp.*; Yuekang Li, Yi Liu, Tianwei Zhang, and Yang Liu, *Nanyang Technological University*; Guo Yu, *China Industrial Control Systems Cyber Emergency Response Team*; Dongjin Wang, *Institute of Scientific and Technical Information, China Academy of Railway Sciences*

## Understanding Communities, Part 2

**“Un-Equal Online Safety?” A Gender Analysis of Security and Privacy Protection Advice and Behaviour Patterns** .. 5611  
Kovila P.L. Coopamootoo, *King’s College London*; Magdalene Ng, *University of Westminster*

**“Millions of people are watching you”:** Understanding the Digital-Safety Needs and Practices of Creators. .... 5629  
Patrawat Samermit, Anna Turner, Patrick Gage Kelley, Tara Matthews, Vanessa Wu, Sunny Consolvo, and Kurt Thomas, *Google*

**How Library IT Staff Navigate Privacy and Security Challenges and Responsibilities** ..... 5647  
Alan F. Luo, Noel Warford, and Samuel Dooley, *University of Maryland*; Rachel Greenstadt, *New York University*; Michelle L. Mazurek, *University of Maryland*; Nora McDonald, *George Mason University*

**Problematic Advertising and its Disparate Exposure on Facebook.** ..... 5665  
Muhammad Ali, *Northeastern University*; Angelica Goetzen, *Max Planck Institute for Software Systems*; Alan Mislove, *Northeastern University*; Elissa M. Redmiles, *Max Planck Institute for Software Systems*; Piotr Sapiiezynski, *Northeastern University*

**One Size Does not Fit All: Quantifying the Risk of Malicious App Encounters for Different Android User Profiles** .. 5683  
Savino Dambra, Leyla Bilge, and Platon Kotzias, *Norton Research Group*; Yun Shen, *NetApp*; Juan Caballero, *IMDEA Software Institute*

## Routing and VPNs

**How Effective is Multiple-Vantage-Point Domain Control Validation?** ..... 5701  
Grace H. Cimaszewski, Henry Birge-Lee, Liang Wang, Jennifer Rexford, and Prateek Mittal, *Princeton University*

**Bypassing Tunnels: Leaking VPN Client Traffic by Abusing Routing Tables.** ..... 5719  
Nian Xue, *New York University*; Yashaswi Malla, Zihang Xia, and Christina Pöpper, *New York University Abu Dhabi*; Mathy Vanhoef, *imec-DistriNet, KU Leuven*

**Back to School: On the (In)Security of Academic VPNs** ..... 5737  
Ka Lok Wu, *The Chinese University of Hong Kong*; Man Hong Hue, *The Chinese University of Hong Kong and Georgia Institute of Technology*; Ngai Man Poon, *The Chinese University of Hong Kong*; Kin Man Leung, *The University of British Columbia*; Wai Yin Po, Kin Ting Wong, Sze Ho Hui, and Sze Yiu Chau, *The Chinese University of Hong Kong*

**FABRID: Flexible Attestation-Based Routing for Inter-Domain Networks** ..... 5755  
Cyrill Krähenbühl, Marc Wyss, and David Basin, *ETH Zürich*; Vincent Lenders, *armasuisse*; Adrian Perrig, *ETH Zürich*; Martin Strohmeier, *armasuisse*

**“All of them claim to be the best”:** Multi-perspective study of VPN users and VPN providers ..... 5773  
Reethika Ramesh, *University of Michigan*; Anjali Vyas, *Cornell Tech*; Roya Ensafi, *University of Michigan*

## Embedded Systems and Firmware

**Greenhouse: Single-Service Rehosting of Linux-Based Firmware Binaries in User-Space Emulation.** ..... 5791  
Hui Jun Tay, Kyle Zeng, Jayakrishna Menon Vadayath, Arvind S Raj, Audrey Dutcher, Tejesh Reddy, Wil Gibbs, Zion Leonahenahe Basque, Fangzhou Dong, Zack Smith, Adam Doupé, Tiffany Bao, Yan Shoshitaishvili, and Ruoyu Wang, *Arizona State University*



**FuncTeller: How Well Does eFPGA Hide Functionality?** ..... 5809  
Zhaokun Han, *Texas A&M University*; Mohammed Shayan, *The University of Texas at Dallas*; Aneesh Dixit, *Texas A&M University*; Mustafa Shihab and Yiorgos Makris, *The University of Texas at Dallas*; Jeyavijayan (JV) Rajendran, *Texas A&M University*

**ACFA: Secure Runtime Auditing & Guaranteed Device Healing via Active Control Flow Attestation** ..... 5827  
Adam Caulfield, *Rochester Institute of Technology*; Norrathep Rattanavipanon, *Prince of Songkla University, Phuket Campus*; Ivan De Oliveira Nunes, *Rochester Institute of Technology*

**Fuzz The Power: Dual-role State Guided Black-box Fuzzing for USB Power Delivery** ..... 5845  
Kyungtae Kim and Sungwoo Kim, *Purdue University*; Kevin R. B. Butler, *University of Florida*; Antonio Bianchi, Rick Kennell, and Dave (Jing) Tian, *Purdue University*

**The Impostor Among US(B): Off-Path Injection Attacks on USB Communications** ..... 5863  
Robert Dumitru, *The University of Adelaide and Defence Science and Technology Group*; Daniel Genkin, *Georgia Tech*; Andrew Wabnitz, *Defence Science and Technology Group*; Yuval Yarom, *The University of Adelaide*

## Attacks on Cryptography

**A comprehensive, formal and automated analysis of the EDHOC protocol** ..... 5881  
Charlie Jacomme, *Inria Paris*; Elise Klein, Steve Kremer, and Maïwenn Racouchot, *Inria Nancy and Université de Lorraine*

**Hash Gone Bad: Automated discovery of protocol attacks that exploit hash function weaknesses** ..... 5899  
Vincent Cheval, *Inria Paris*; Cas Cremers and Alexander Dax, *CISPA Helmholtz Center for Information Security*; Lucca Hirschi, *Inria & LORIA*; Charlie Jacomme, *Inria Paris*; Steve Kremer, *Université de Lorraine, LORIA, Inria Nancy Grand-Est*

**How fast do you heal? A taxonomy for post-compromise security in secure-channel establishment** ..... 5917  
Olivier Blazy, *LIX, CNRS, Inria, École Polytechnique, Institut Polytechnique de Paris, France*; Ioana Boureanu, *University of Surrey, Surrey Centre for Cyber Security, UK*; Pascal Lafourcade, *LIMOS, University of Clermont Auvergne, France*; Cristina Onete, *XLIM, University of Limoges, France*; Léo Robert, *LIMOS, University of Clermont Auvergne, France*

**Automated Analysis of Protocols that use Authenticated Encryption: How Subtle AEAD Differences can impact Protocol Security** ..... 5935  
Cas Cremers, *CISPA Helmholtz Center for Information Security*; Alexander Dax, *CISPA Helmholtz Center for Information Security and Saarland University*; Charlie Jacomme, *Inria Paris*; Mang Zhao, *CISPA Helmholtz Center for Information Security and Saarland University*

**High Recovery with Fewer Injections: Practical Binary Volumetric Injection Attacks against Dynamic Searchable Encryption** ..... 5953  
Xianglong Zhang and Wei Wang, *Huazhong University of Science and Technology*; Peng Xu, *Huazhong University of Science and Technology and Hubei Key Laboratory of Distributed System Security*; Laurence T. Yang, *Huazhong University of Science and Technology and St. Francis Xavier University*; Kaitai Liang, *Delft University of Technology*

## Cloud Insecurity

**Cross Container Attacks: The Bewildered eBPF on Clouds** ..... 5971  
Yi He and Roland Guo, *Tsinghua University and BNRist*; Yunlong Xing, *George Mason University*; Xijia Che, *Tsinghua University and BNRist*; Kun Sun, *George Mason University*; Zhuotao Liu, Ke Xu, and Qi Li, *Tsinghua University*

**DScope: A Cloud-Native Internet Telescope** ..... 5989  
Eric Pauley, Paul Barford, and Patrick McDaniel, *University of Wisconsin–Madison*

**Credit Karma: Understanding Security Implications of Exposed Cloud Services through Automated Capability Inference** ..... 6007  
Xueqiang Wang, *University of Central Florida*; Yuqiong Sun, *Meta*; Susanta Nanda, *ServiceNow*; XiaoFeng Wang, *Indiana University Bloomington*

**Detecting Multi-Step IAM Attacks in AWS Environments via Model Checking** ..... 6025  
Ilia Shevrin, *Citi*; Oded Margalit, *Ben-Gurion University*

**Remote Direct Memory Introspection** ..... 6043  
Hongyi Liu, Jiarong Xing, and Yibo Huang, *Rice University*; Danyang Zhuo, *Duke University*; Srinivas Devadas, *Massachusetts Institute of Technology*; Ang Chen, *Rice University*

## More Web and Mobile Security

**Auditing Framework APIs via Inferred App-side Security Specifications** ..... 6061  
Parjanya Vyas, Asim Waheed, Yousra Aafer, and N. Asokan, *University of Waterloo*

**WHIP: Improving Static Vulnerability Detection in Web Application by Forcing tools to Collaborate** ..... 6079  
Feras Al-Kassar, *EURECOM*; Luca Compagna, *SAP Security Research*; Davide Balzarotti, *EURECOM*

**SQRL: Grey-Box Detection of SQL Injection Vulnerabilities Using Reinforcement Learning** ..... 6097  
Salim Al Wahaibi, Myles Foley, and Sergio Maffei, *Imperial College London*

**Hiding in Plain Sight: An Empirical Study of Web Application Abuse in Malware** ..... 6115  
Mingxuan Yao, *Georgia Institute of Technology*; Jonathan Fuller, *United States Military Academy*; Ranjita Pai Kasturi, Saumya Agarwal, Amit Kumar Sikder, and Brendan Saltaformaggio, *Georgia Institute of Technology*

**Bilingual Problems: Studying the Security Risks Incurred by Native Extensions in Scripting Languages** ..... 6133  
Cristian-Alexandru Staicu, *CISPA Helmholtz Center for Information Security*; Sazzadur Rahaman, *University of Arizona*; Ágnes Kiss and Michael Backes, *CISPA Helmholtz Center for Information Security*

## Networks and Security

**Did the Shark Eat the Watchdog in the NTP Pool? Deceiving the NTP Pool's Monitoring System** ..... 6151  
Jonghoon Kwon, *ETH Zürich*; Jeonggyu Song and Junbeom Hur, *Korea University*; Adrian Perrig, *ETH Zürich*

**Device Tracking via Linux's New TCP Source Port Selection Algorithm** ..... 6167  
Moshe Kol, Amit Klein, and Yossi Gilad, *Hebrew University of Jerusalem*

**Temporal CDN-Convex Lens: A CDN-Assisted Practical Pulsing DDoS Attack** ..... 6185  
Run Guo, *Tsinghua University*; Jianjun Chen, *Tsinghua University and Zhongguancun Laboratory*; Yihang Wang and Keran Mu, *Tsinghua University*; Baojun Liu, *Tsinghua University and Zhongguancun Laboratory*; Xiang Li, *Tsinghua University*; Chao Zhang, *Tsinghua University and Zhongguancun Laboratory*; Haixin Duan, *Tsinghua University and Zhongguancun Laboratory and QI-ANXIN Technology Research Institute*; Jianping Wu, *Tsinghua University and Zhongguancun Laboratory*

**An Efficient Design of Intelligent Network Data Plane** ..... 6203  
Guangmeng Zhou, *Tsinghua University*; Zhuotao Liu, *Tsinghua University and Zhongguancun Laboratory*; Chuanpu Fu, *Tsinghua University*; Qi Li and Ke Xu, *Tsinghua University and Zhongguancun Laboratory*

**Glowing in the Dark: Uncovering IPv6 Address Discovery and Scanning Strategies in the Wild** ..... 6221  
Hamas Bin Tanveer, *The University of Iowa*; Rachee Singh, *Microsoft and Cornell University*; Paul Pearce, *Georgia Tech*; Rishab Nithyanand, *University of Iowa*

## Arming and Disarming ARM

**Oops..! I Glitched It Again! How to Multi-Glitch the Glitching-Protections on ARM TrustZone-M** ..... 6239  
Xhani Marvin Saß, Richard Mitev, and Ahmad-Reza Sadeghi, *Technical University of Darmstadt*

**SHELTER: Extending Arm CCA with Isolation in User Space** ..... 6257  
Yiming Zhang, *Southern University of Science and Technology and The Hong Kong Polytechnic University*; Yuxin Hu, *Southern University of Science and Technology*; Zhenyu Ning, *Hunan University and Southern University of Science and Technology*; Fengwei Zhang, *Southern University of Science and Technology*; Xiapu Luo, *The Hong Kong Polytechnic University*; Haoyang Huang, *Southern University of Science and Technology*; Shoumeng Yan and Zhengyu He, *Ant Group*

**Hot Pixels: Frequency, Power, and Temperature Attacks on GPUs and Arm SoCs** ..... 6275  
Hritvik Taneja, Jason Kim, and Jie Jeff Xu, *Georgia Tech*; Stephan van Schaik, *University of Michigan*; Daniel Genkin, *Georgia Tech*; Yuval Yarom, *Ruhr University Bochum*

**SPECTREM: Exploiting Electromagnetic Emanations During Transient Execution** ..... 6293  
Jesse De Meulemeester, Antoon Purnal, Lennert Wouters, Arthur Beckers, and Ingrid Verbauwhede, *COSIC, KU Leuven*

<b>ARMORE: Pushing Love Back Into Binaries</b> .....	<b>6311</b>
Luca Di Bartolomeo, Hossein Moghaddas, and Mathias Payer, <i>EPFL</i>	
<b>More ML Attacks and Defenses</b>	
<b>Secure Floating-Point Training</b> .....	<b>6329</b>
Deevashwer Rathee, <i>University of California, Berkeley</i> ; Anwesh Bhattacharya, Divya Gupta, and Rahul Sharma, <i>Microsoft Research</i> ; Dawn Song, <i>University of California, Berkeley</i>	
<b>NeuroPots: Realtime Proactive Defense against Bit-Flip Attacks in Neural Networks</b> .....	<b>6347</b>
Qi Liu, <i>Lehigh University</i> ; Jieming Yin, <i>Nanjing University of Posts and Telecommunications</i> ; Wujie Wen, <i>Lehigh University</i> ; Chengmo Yang, <i>University of Delaware</i> ; Shi Sha, <i>Wilkes University</i>	
<b>FedVal: Different good or different bad in federated learning</b> .....	<b>6365</b>
Viktor Valadi, <i>AI Sweden</i> ; Xinchu Qiu, Pedro Porto Buarque de Gusmão, and Nicholas D. Lane, <i>University of Cambridge</i> ; Mina Alibeigi, <i>University of Cambridge and Zenseact AB</i>	
<b>Gradient Obfuscation Gives a False Sense of Security in Federated Learning</b> .....	<b>6381</b>
Kai Yue, <i>North Carolina State University</i> ; Richeng Jin, <i>Zhejiang University</i> ; Chau-Wai Wong, Dror Baron, and Huaiyu Dai, <i>North Carolina State University</i>	
<b>FREEEAGLE: Detecting Complex Neural Trojans in Data-Free Cases</b> .....	<b>6399</b>
Chong Fu, Xuhong Zhang, and Shouling Ji, <i>Zhejiang University</i> ; Ting Wang, <i>Pennsylvania State University</i> ; Peng Lin, <i>Chinese Aeronautical Establishment</i> ; Yanghe Feng, <i>National University of Defense Technology</i> ; Jianwei Yin, <i>Zhejiang University</i>	
<b>Cryptography for Privacy</b>	
<b>Prime Match: A Privacy-Preserving Inventory Matching System</b> .....	<b>6417</b>
Antigoni Polychroniadou, <i>J.P. Morgan</i> ; Gilad Asharov, <i>Bar-Ilan University</i> ; Benjamin Diamond, Tucker Balch, Hans Buehler, Richard Hua, Suwen Gu, Greg Gimler, and Manuela Veloso, <i>J.P. Morgan</i>	
<b>Squirrel: A Scalable Secure Two-Party Computation Framework for Training Gradient Boosting Decision Tree</b>	<b>6435</b>
Wen-jie Lu and Zhicong Huang, <i>Alibaba Group</i> ; Qizhi Zhang, <i>Ant Group</i> ; Yuchen Wang, <i>Alibaba Group</i> ; Cheng Hong, <i>Ant Group</i>	
<b>Eos: Efficient Private Delegation of zkSNARK Provers</b> .....	<b>6453</b>
Alessandro Chiesa, <i>UC Berkeley and EPFL</i> ; Ryan Lehmkuhl, <i>MIT</i> ; Pratyush Mishra, <i>Aleo and University of Pennsylvania</i> ; Yinuo Zhang, <i>UC Berkeley</i>	
<b>Machine-checking Multi-Round Proofs of Shuffle: Terelius-Wikstrom and Bayer-Groth</b> .....	<b>6471</b>
Thomas Haines, <i>Australian National University</i> ; Rajeev Gore, <i>Polish Academy of Science</i> ; Mukesh Tiwari, <i>University of Cambridge</i>	
<b>TAP: Transparent and Privacy-Preserving Data Services</b> .....	<b>6489</b>
Daniel Reijnders and Aung Maw, <i>Singapore University of Technology and Design</i> ; Zheng Yang, <i>Southwest University</i> ; Tien Tuan Anh Dinh and Jianying Zhou, <i>Singapore University of Technology and Design</i>	
<b>Vulnerabilities and Threat Detection</b>	
<b>Trojan Source: Invisible Vulnerabilities</b> .....	<b>6507</b>
Nicholas Boucher, <i>University of Cambridge</i> ; Ross Anderson, <i>University of Cambridge and University of Edinburgh</i>	
<b>Cheesecloth: Zero-Knowledge Proofs of Real World Vulnerabilities</b> .....	<b>6525</b>
Santiago Cuéllar, Bill Harris, James Parker, and Stuart Pernsteiner, <i>Galois, Inc.</i> ; Eran Tromer, <i>Columbia University</i>	
<b>VISCAN: Discovering 1-day Vulnerabilities in Reused C/C++ Open-source Software Components Using Code Classification Techniques</b> .....	<b>6541</b>
Seunghoon Woo, Eunjin Choi, Heejo Lee, and Hakjoo Oh, <i>Korea University</i>	
<b>VulChecker: Graph-based Vulnerability Localization in Source Code</b> .....	<b>6557</b>
Yisroel Mirsky, <i>Ben-Gurion University of the Negev</i> ; George Macon, <i>Georgia Tech Research Institute</i> ; Michael Brown, <i>Georgia Institute of Technology</i> ; Carter Yagemann, <i>Ohio State University</i> ; Matthew Pruett, Evan Downing, Sukarno Mertoguno, and Wenke Lee, <i>Georgia Institute of Technology</i>	

**DISTDET: A Cost-Effective Distributed Cyber Threat Detection System** . . . . . 6575  
Feng Dong, *School of Cyber Science and Engineering, Huazhong University of Science and Technology / Sangfor Technologies Inc.*; Liu Wang and Xu Nie, *Beijing University of Posts and Telecommunications*; Fei Shao, *Case Western Reserve University*; Haoyu Wang, *School of Cyber Science and Engineering, Huazhong University of Science and Technology*; Ding Li, *Key Laboratory of High-Confidence Software Technologies (MOE), School of Computer Science, Peking University*; Xiapu Luo, *The Hong Kong Polytechnic University*; Xusheng Xiao, *Arizona State University*

## **Automated Analysis of Deployed Systems**

**Automated Security Analysis of Exposure Notification Systems** . . . . . 6593  
Kevin Morio and Ilkan Esiyok, *CISPA Helmholtz Center for Information Security*; Dennis Jackson, *Mozilla*; Robert Künnemann, *CISPA Helmholtz Center for Information Security*

**Formal Analysis of SPDM: Security Protocol and Data Model version 1.2** . . . . . 6611  
Cas Cremers, Alexander Dax, and Aurora Naska, *CISPA Helmholtz Center for Information Security*

**One Size Does Not Fit All: Uncovering and Exploiting Cross Platform Discrepant APIs in WeChat** . . . . . 6629  
Chao Wang, Yue Zhang, and Zhiqiang Lin, *The Ohio State University*

**The Most Dangerous Codec in the World: Finding and Exploiting Vulnerabilities in H.264 Decoders** . . . . . 6647  
Willy R. Vasquez, *The University of Texas at Austin*; Stephen Checkoway, *Oberlin College*; Hovav Shacham, *The University of Texas at Austin*

**Are You Spying on Me? Large-Scale Analysis on IoT Data Exposure through Companion Apps** . . . . . 6665  
Yuhong Nan, *Sun Yat-sen University*; Xueqiang Wang, *University of Central Florida*; Luyi Xing and Xiaojing Liao, *Indiana University Bloomington*; Ruoyu Wu and Jianliang Wu, *Purdue University*; Yifan Zhang and XiaoFeng Wang, *Indiana University Bloomington*

## **Manipulation, Influence, and Elections**

**Strategies and Vulnerabilities of Participants in Venezuelan Influence Operations** . . . . . 6683  
Ruben Recabarren, Bogdan Carbutar, Nestor Hernandez, and Ashfaq Ali Shafin, *Florida International University*

**TRIDENT: Towards Detecting and Mitigating Web-based Social Engineering Attacks** . . . . . 6701  
Zheng Yang, Joey Allen, and Matthew Landen, *Georgia Institute of Technology*; Roberto Perdisci, *Georgia Tech and University of Georgia*; Wenke Lee, *Georgia Institute of Technology*

**Fact-Saboteurs: A Taxonomy of Evidence Manipulation Attacks against Fact-Verification Systems** . . . . . 6719  
Sahar Abdelnabi and Mario Fritz, *CISPA Helmholtz Center for Information Security*

**Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol** . . . . . 6737  
Alexandre Debant and Lucca Hirschi, *Université de Lorraine, Inria, CNRS, France*

**PROVIDENCE: a Flexible Round-by-Round Risk-Limiting Audit** . . . . . 6753  
Oliver Broadrick and Poorvi Vora, *The George Washington University*; Filip Zagórski, *University of Wroclaw and Votifica*

## **Side Channel Attacks**

**NVLeak: Off-Chip Side-Channel Attacks via Non-Volatile Memory Systems** . . . . . 6771  
Zixuan Wang, *UC San Diego*; Mohammadkazem Taram, *Purdue University and UC San Diego*; Daniel Moghimi, *UT Austin and UC San Diego*; Steven Swanson, Dean Tullsen, and Jishen Zhao, *UC San Diego*

**Cipherfix: Mitigating Ciphertext Side-Channel Attacks in Software** . . . . . 6789  
Jan Wichelmann, Anna Pätschke, Luca Wilke, and Thomas Eisenbarth, *University of Lübeck*

**Side-Channel Attacks on Optane Persistent Memory** . . . . . 6807  
Sihang Liu, *University of Virginia*; Suraj Kanniwadi, *Cornell University*; Martin Schwarzl, Andreas Kogler, and Daniel Gruss, *Graz University of Technology*; Samira Khan, *University of Virginia*

**PSPRAY: Timing Side-Channel based Linux Kernel Heap Exploitation Technique** . . . . . 6825  
Yoochan Lee and Jinhan Kwak, *Seoul National University*; Junesoo Kang and Yuseok Jeon, *UNIST*; Byoungyoung Lee, *Seoul National University*

**CIPHERH: Automated Detection of Ciphertext Side-channel Vulnerabilities in Cryptographic Implementations . . . 6843**  
Sen Deng, *Southern University of Science and Technology*; Mengyuan Li, *The Ohio State University*; Yining Tang, *Southern University of Science and Technology*; Shuai Wang, *Hong Kong University of Science and Technology*; Shoumeng Yan, *The Ant Group*; Yinqian Zhang, *Southern University of Science and Technology*

## Transportation and Infrastructure

**ICSPatch: Automated Vulnerability Localization and Non-Intrusive Hotpatching in Industrial Control Systems using Data Dependence Graphs. . . . . 6861**  
Prashant Hari Narayan Rajput, *NYU Tandon School of Engineering*; Constantine Dourmanidis and Michail Maniatakos, *New York University Abu Dhabi*

**Access Denied: Assessing Physical Risks to Internet Access Networks. . . . . 6877**  
Alexander Marder, *CAIDA / UC San Diego*; Zesen Zhang, *UC San Diego*; Ricky Mok and Ramakrishna Padmanabhan, *CAIDA / UC San Diego*; Bradley Huffaker, *CAIDA / UC San Diego*; Matthew Luckie, *University of Waikato*; Alberto Dainotti, *Georgia Tech*; kc claffy, *CAIDA / UC San Diego*; Alex C. Snoeren and Aaron Schulman, *UC San Diego*

**ZBCAN: A Zero-Byte CAN Defense System. . . . . 6893**  
Khaled Serag, Rohit Bhatia, Akram Faqih, and Muslum Ozgur Ozmen, *Purdue University*; Vireshwar Kumar, *Indian Institute of Technology, Delhi*; Z. Berkay Celik and Dongyan Xu, *Purdue University*

**RIDAS: Real-time identification of attack sources on controller area networks . . . . . 6911**  
Jiwoo Shin and Hyunghoon Kim, *Soongsil University*; Seyoung Lee, Wonsuk Choi, and Dong Hoon Lee, *Korea University*; Hyo Jin Jo, *Soongsil University*

**That Person Moves Like A Car: Misclassification Attack Detection for Autonomous Systems Using Spatiotemporal Consistency. . . . . 6929**  
Yanmao Man, *University of Arizona*; Raymond Muller, *Purdue University*; Ming Li, *University of Arizona*; Z. Berkay Celik, *Purdue University*; Ryan Gerdes, *Virginia Tech*

## Language-Based Security

**TRUST: A Compilation Framework for In-process Isolation to Protect Safe Rust against Untrusted Code . . . . . 6947**  
Inyoung Bang and Martin Kayondo, *Seoul National University*; Hyungon Moon, *UNIST (Ulsan National Institute of Science and Technology)*; Yunheung Paek, *Seoul National University*

**Jinn: Hijacking Safe Programs with Trojans . . . . . 6965**  
Komail Dharsee and John Criswell, *University of Rochester*

**ARGUS: A Framework for Staged Static Taint Analysis of GitHub Workflows and Actions . . . . . 6983**  
Siddharth Muralee, *Purdue University*; Igibek Koishybayev, Aleksandr Nahapetyan, Greg Tystahl, and Brad Reaves, *North Carolina State University*; Antonio Bianchi, *Purdue University*; William Enck and Alexandros Kapravelos, *North Carolina State University*; Aravind Machiry, *Purdue University*

**McFIL: Model Counting Functionality-Inherent Leakage . . . . . 7001**  
Maximilian Zinkus, Yinzhi Cao, and Matthew D. Green, *Johns Hopkins University*

**Extracting Protocol Format as State Machine via Controlled Static Loop Analysis. . . . . 7019**  
Qingkai Shi, Xiangzhe Xu, and Xiangyu Zhang, *Purdue University*

## Browsers

**Isolated and Exhausted: Attacking Operating Systems via Site Isolation in the Browser . . . . . 7037**  
Matthias Gierlings, Marcus Brinkmann, and Jörg Schwenk, *Ruhr University Bochum*

**Extending a Hand to Attackers: Browser Privilege Escalation Attacks via Extensions . . . . . 7055**  
Young Min Kim and Byoungyoung Lee, *Seoul National University*

**RøB: Ransomware over Modern Web Browsers . . . . . 7073**  
Harun Oz, Ahmet Aris, and Abbas Acar, *Cyber-Physical Systems Security Lab, Florida International University*; Güliz Seray Tuncay, *Google*; Leonardo Babun and Selcuk Uluagac, *Cyber-Physical Systems Security Lab, Florida International University*

**Pool-Party: Exploiting Browser Resource Pools for Web Tracking** ..... 7091  
Peter Snyder, *Brave Software*; Soroush Karami, *University of Illinois at Chicago*; Arthur Edelstein, *Brave Software*;  
Benjamin Livshits, *Imperial College London*; Hamed Haddadi, *Brave Software and Imperial College of London*

**Checking Passwords on Leaky Computers: A Side Channel Analysis of Chrome’s Password Leak Detect Protocol** .. 7107  
Andrew Kwong, *UNC Chapel Hill*; Walter Wang, *University of Michigan*; Jason Kim, *Georgia Tech*; Jonathan Berger,  
*Bar Ilan University*; Daniel Genkin, *Georgia Tech*; Eyal Ronen, *Tel Aviv University*; Hovav Shacham, *UT Austin*;  
Riad Wahby, *CMU*; Yuval Yarom, *Ruhr University Bochum*

## **Speculation Doesn’t Pay**

**Ultimate SLH: Taking Speculative Load Hardening to the Next Level** ..... 7125  
Zhiyuan Zhang, *The University of Adelaide*; Gilles Barthe, *MPI-SP and IMDEA Software Institute*;  
Chitchanok Chuengsatiansup, *The University of Melbourne*; Peter Schwabe, *MPI-SP and Radboud University*;  
Yuval Yarom, *The University of Adelaide*

**Speculation at Fault: Modeling and Testing Microarchitectural Leakage of CPU Exceptions** ..... 7143  
Jana Hofmann, *Azure Research, Microsoft*; Emanuele Vannacci, *Vrije Universiteit Amsterdam*; Cédric Fournet,  
Boris Köpf, and Oleksii Oleksenko, *Azure Research, Microsoft*

**PROSPECT: Provably Secure Speculation for the Constant-Time Policy** ..... 7161  
Lesly-Ann Daniel, Marton Bognar, and Job Noorman, *imec-DistriNet, KU Leuven*; Sébastien Bardin, *CEA, LIST*,  
*Université Paris Saclay*; Tamara Rezk, *INRIA, Université Côte d’Azur, Sophia Antipolis*; Frank Piessens, *imec-DistriNet*,  
*KU Leuven*

**Downfall: Exploiting Speculative Data Gathering** ..... 7179  
Daniel Moghimi, *UCSD*

## **Facing the Facts**

**FACE-AUDITOR: Data Auditing in Facial Recognition Systems** ..... 7195  
Min Chen, *CISPA Helmholtz Center for Information Security*; Zhikun Zhang, *CISPA Helmholtz Center for*  
*Information Security and Stanford University*; Tianhao Wang, *University of Virginia*; Michael Backes and  
Yang Zhang, *CISPA Helmholtz Center for Information Security*

**UnGANable: Defending Against GAN-based Face Manipulation** ..... 7213  
Zheng Li, *CISPA Helmholtz Center for Information Security*; Ning Yu, *Salesforce Research*; Ahmed Salem,  
*Microsoft Research*; Michael Backes, Mario Fritz, and Yang Zhang, *CISPA Helmholtz Center for Information Security*

**Fairness Properties of Face Recognition and Obfuscation Systems** ..... 7231  
Harrison Rosenberg, *University of Wisconsin–Madison*; Brian Tang, *University of Michigan*; Kassem Fawaz and  
Somesh Jha, *University of Wisconsin–Madison*

**GlitchHiker: Uncovering Vulnerabilities of Image Signal Transmission with IEMI** ..... 7249  
Qinhong Jiang, Xiaoyu Ji, Chen Yan, Zhixin Xie, Haina Lou, and Wenyuan Xu, *Zhejiang University*

## **More Hardware Side Channels**

**(M)WAIT for It: Bridging the Gap between Microarchitectural and Architectural Side Channels** ..... 7267  
Ruiyi Zhang, *CISPA Helmholtz Center for Information Security*; Taehyun Kim, *Independent*; Daniel Weber and  
Michael Schwarz, *CISPA Helmholtz Center for Information Security*

**Collide+Power: Leaking Inaccessible Data with Software-based Power Side Channels** ..... 7285  
Andreas Kogler, Jonas Juffinger, and Lukas Giner, *Graz University of Technology*; Lukas Gerlach, *CISPA Helmholtz*  
*Center for Information Security*; Martin Schwarzl, *Graz University of Technology*; Michael Schwarz, *CISPA Helmholtz*  
*Center for Information Security*; Daniel Gruss and Stefan Mangard, *Graz University of Technology*

**INCEPTION: Exposing New Attack Surfaces with Training in Transient Execution** ..... 7303  
Daniël Trujillo, Johannes Wikner, and Kaveh Razavi, *ETH Zurich*

**BunnyHop: Exploiting the Instruction Prefetcher** ..... 7321  
Zhiyuan Zhang, Mingtian Tao, and Sioli O’Connell, *The University of Adelaide*; Chitchanok Chuengsatiansup,  
*The University of Melbourne*; Daniel Genkin, *Georgia Tech*; Yuval Yarom, *The University of Adelaide*

## Deeper Thoughts on Deep Learning

**Can a Deep Learning Model for One Architecture Be Used for Others? Retargeted-Architecture Binary Code Analysis** ..... 7339  
Junzhe Wang, *George Mason University*; Matthew Sharp, *University of South Carolina*; Chuxiong Wu, Qiang Zeng, and Lannan Luo, *George Mason University*

**Decompiling x86 Deep Neural Network Executables** ..... 7357  
Zhibo Liu, Yuanyuan Yuan, and Shuai Wang, *The Hong Kong University of Science and Technology*; Xiaofei Xie, *Singapore Management University*; Lei Ma, *University of Alberta*

**AIRS: Explanation for Deep Reinforcement Learning based Security Applications** ..... 7375  
Jiahao Yu, *Northwestern University*; Wenbo Guo, *Purdue University*; Qi Qin, *ShanghaiTech University*; Gang Wang, *University of Illinois at Urbana-Champaign*; Ting Wang, *The Pennsylvania State University*; Xinyu Xing, *Northwestern University*

**Differential Testing of Cross Deep Learning Framework APIs: Revealing Inconsistencies and Vulnerabilities** . . . . 7393  
Zizhuang Deng, Guozhu Meng, Kai Chen, Tong Liu, and Lu Xiang, *SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, China*; *School of Cyber Security, University of Chinese Academy of Sciences, China*; Chunyang Chen, *Monash University, Australia*

## Attacks on Deployed Cryptosystems

**Every Signature is Broken: On the Insecurity of Microsoft Office's OOXML Signatures** ..... 7411  
Simon Rohlmann, Vladislav Mladenov, Christian Mainka, Daniel Hirschberger, and Jörg Schwenk, *Ruhr University Bochum*

**Downgrading DNSSEC: How to Exploit Crypto Agility for Hijacking Signed Zones** ..... 7429  
Elias Heftrig, *ATHENE and Fraunhofer SIT*; Haya Shulman, *ATHENE, Fraunhofer SIT, and Goethe-Universität Frankfurt*; Michael Waidner, *ATHENE, Fraunhofer SIT, and Technische Universität Darmstadt*

**Security Analysis of MongoDB Queryable Encryption** ..... 7445  
Zichen Gui, Kenneth G. Paterson, and Tianxin Tang, *ETH Zurich*

**All cops are broadcasting: TETRA under scrutiny** ..... 7463  
Carlo Meijer, Wouter Bokslag, and Jos Wetzels, *Midnight Blue*

## Attacking, Defending, and Analyzing

**On the Feasibility of Malware Unpacking via Hardware-assisted Loop Profiling** ..... 7481  
Binlin Cheng, *Shandong University*; Erika A Leal, *Tulane University*; Haotian Zhang, *The University of Texas at Arlington*; Jiang Ming, *Tulane University*

**Multiview: Finding Blind Spots in Access-Deny Issues Diagnosis** ..... 7499  
Bingyu Shen, Tianyi Shan, and Yuanyuan Zhou, *University of California, San Diego*

**Attacks are Forwarded: Breaking the Isolation of MicroVM-based Containers Through Operation Forwarding** . . . 7517  
Jietao Xiao and Nanzi Yang, *State Key Lab of ISN, School of Cyber Engineering, Xidian University, China*; Wenbo Shen, *Zhejiang University, China*; Jinku Li and Xin Guo, *State Key Lab of ISN, School of Cyber Engineering, Xidian University, China*; Zhiqiang Dong and Fei Xie, *Tencent Security Yunding Lab, China*; Jianfeng Ma, *State Key Lab of ISN, School of Cyber Engineering, Xidian University, China*

**AutoFR: Automated Filter Rule Generation for Adblocking** ..... 7535  
Hieu Le, Salma Elmalaki, and Athina Markopoulou, *University of California, Irvine*; Zubair Shafiq, *University of California, Davis*