33rd USENIX Security Symposium

August 14–16, 2024
Philadelphia, PA, USA

Wednesday, August 14

User Studies I: Social Media Platforms

"I feel physically safe but not politically safe": Understanding the Digital Threats and Safety Practices of OnlyFans Creators 1
Ananta Soneji, *Arizona State University;* Vaughn Hamilton, *Max Planck Institute for Software Systems;* Adam Doupé, *Arizona State University;* Allison McDonald, *Boston University;* Elissa M. Redmiles, *Georgetown University*

"I chose to fight, be brave, and to deal with it": Threat Experiences and Security Practices of Pakistani Content Creators 19
Lea Gröber, *CISPA Helmholtz Center for Information Security and Saarland University;* Waleed Arshad and Shanza, *Lahore University of Management Sciences;* Angelica Goetzen, *Max Planck Institute for Software Systems;* Elissa M. Redmiles, *Georgetown University;* Maryam Mustafa, *Lahore University of Management Sciences;* Katharina Krombholz, *CISPA Helmholtz Center for Information Security*

Investigating Moderation Challenges to Combating Hate and Harassment: The Case of Mod-Admin Power Dynamics and Feature Misuse on Reddit 37
Madiha Tabassum, *Northeastern University;* Alana Mackey, *Wellesley College;* Ashley Schuett, *George Washington University;* Ada Lerner, *Northeastern University*

"Did They F*ing Consent to That?": Safer Digital Intimacy via Proactive Protection Against Image-Based Sexual Abuse 55**
Lucy Qin, *Georgetown University;* Vaughn Hamilton, *Max Planck Institute for Software Systems;* Sharon Wang, *University of Washington;* Yigit Aydinalp and Marin Scarlett, *European Sex Workers Rights Alliance;* Elissa M. Redmiles, *Georgetown University*

Hardware Security I: Attacks and Defense

***AttackGNN*: Red-Teaming GNNs in Hardware Security Using Reinforcement Learning 73**
Vasudev Gohil, *Texas A&M University;* Satwik Patnaik, *University of Delaware;* Dileep Kalathil and Jeyavijayan Rajendran, *Texas A&M University*

INSIGHT: Attacking Industry-Adopted Learning Resilient Logic Locking Techniques Using Explainable Graph Neural Network 91
Lakshmi Likhitha Mankali, *New York University;* Ozgur Sinanoglu, *New York University Abu Dhabi;* Satwik Patnaik, *University of Delaware*

Eye of Sauron: Long-Range Hidden Spy Camera Detection and Positioning with Inbuilt Memory EM Radiation . . . 109
Qibo Zhang and Daibo Liu, *Hunan University;* Xinyu Zhang, *University of California San Diego;* Zhichao Cao, *Michigan State University;* Fanzi Zeng, Hongbo Jiang, and Wenqiang Jin, *Hunan University*

Improving the Ability of Thermal Radiation Based Hardware Trojan Detection 127
Ting Su, Yaohua Wang, Shi Xu, Lusi Zhang, Simin Feng, Jialong Song, Yiming Liu, Yongkang Tang, Yang Zhang, Shaoqing Li, Yang Guo, and Hengzhu Liu, *National University of Defense Technology*

System Security I: OS

Endokernel: A Thread Safe Monitor for Lightweight Subprocess Isolation 145
Fangfei Yang, *Rice University;* Bumjin Im, *Amazon.com;* Weijie Huang, *Rice University;* Kelly Kaoudis, *Trail of Bits;* Anjo Vahldiek-Oberwagner, *Intel Labs;* Chia-Che Tsai, *Texas A&M University;* Nathan Dautenhahn, *Riverside Research*

HIVE: A Hardware-assisted Isolated Execution Environment for eBPF on AArch64 163
Peihua Zhang, *SKLP, Institute of Computing Technology, CAS; University of Chinese Academy of Sciences;* Chenggang Wu, *SKLP, Institute of Computing Technology, CAS; University of Chinese Academy of Sciences; Zhongguancun Laboratory;* Xiangyu Meng, *Northwestern Polytechnical University;* Yinqian Zhang, *Southern University of Science and Technology;* Mingfan Peng, Shiyang Zhang, and Bing Hu, *SKLP, Institute of Computing Technology, CAS; University of Chinese Academy of Sciences;* Mengyao Xie, *SKLP, Institute of Computing Technology, CAS;* Yuanming Lai and Yan Kang, *SKLP, Institute of Computing Technology, CAS; University of Chinese Academy of Sciences;* Zhe Wang, *SKLP, Institute of Computing Technology, CAS; University of Chinese Academy of Sciences; Zhongguancun Laboratory*

BUDAlloc: Defeating Use-After-Free Bugs by Decoupling Virtual Address Management from Kernel 181
Junho Ahn, Jaehyeon Lee, Kanghyuk Lee, Wooseok Gwak, Minseong Hwang, and Youngjin Kwon, *KAIST*

Page-Oriented Programming: Subverting Control-Flow Integrity of Commodity Operating System Kernels with Non-Writable Code Pages 199
Seunghun Han, *The Affiliated Institute of ETRI, Chungnam National University;* Seong-Joong Kim, Wook Shin, and Byung Joon Kim, *The Affiliated Institute of ETRI;* Jae-Cheol Ryou, *Chungnam National University*

Network Security I: DDoS

SMARTCOOKIE: Blocking Large-Scale SYN Floods with a Split-Proxy Defense on Programmable Data Planes 217
Sophia Yoo, Xiaoqi Chen, and Jennifer Rexford, *Princeton University*

Loopy Hell(ow): Infinite Traffic Loops at the Application Layer 235
Yepeng Pan, Anna Ascheman, and Christian Rossow, *CISPA Helmholtz Center for Information Security*

Zero-setup Intermediate-rate Communication Guarantees in a Global Internet 253
Marc Wyss and Adrian Perrig, *ETH Zurich*

Towards an Effective Method of ReDoS Detection for Non-backtracking Engines. 271
Weihao Su, Hong Huang, and Rongchen Li, *Key Laboratory of System Software* (*Chinese Academy of Sciences*) *and State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences; University of Chinese Academy of Sciences;* Haiming Chen, *Key Laboratory of System Software* (*Chinese Academy of Sciences*) *and State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences;* Tingjian Ge, *Miner School of Computer & Information Sciences, University of Massachusetts, Lowell*

ML I: Federated Learning

FAMOS: Robust Privacy-Preserving Authentication on Payment Apps via Federated Multi-Modal Contrastive Learning 289
Yifeng Cai, *Key Laboratory of High Confidence Software Technologies* (*PKU*), *Ministry of Education; School of Computer Science, Peking University;* Ziqi Zhang, *Department of Computer Science, University of Illinois Urbana-Champaign;* Jiaping Gui, *School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University;* Bingyan Liu, *School of Computer Science, Beijing University of Posts and Telecommunications;* Xiaoke Zhao, Ruoyu Li, and Zhe Li, *Ant Group;* Ding Li, *Key Laboratory of High Confidence Software Technologies* (*PKU*), *Ministry of Education; School of Computer Science, Peking University*

Efficient Privacy Auditing in Federated Learning 307
Hongyan Chang, *National University of Singapore;* Brandon Edwards, *Intel Corporation;* Anindya S. Paul, *University of Florida;* Reza Shokri, *National University of Singapore*

Defending Against Data Reconstruction Attacks in Federated Learning: An Information Theory Approach 325
Qi Tan, *Department of Computer Science and Technology, Tsinghua University;* Qi Li, *Institute for Network Science and Cyberspace, Tsinghua University;* Yi Zhao, *School of Cyberspace Science and Technology, Beijing Institute of Technology;* Zhuotao Liu, *Institute for Network Science and Cyberspace, Tsinghua University;* Xiaobing Guo, *Lenovo Research;* Ke Xu, *Department of Computer Science and Technology, Tsinghua University*

Lotto: Secure Participant Selection against Adversarial Servers in Federated Learning 343
Zhifeng Jiang and Peng Ye, *Hong Kong University of Science and Technology;* Shiqi He, *University of Michigan;* Wei Wang, *Hong Kong University of Science and Technology;* Ruichuan Chen, *Nokia Bell Labs;* Bo Li, *Hong Kong University of Science and Technology*

Security Analysis I: Source Code and Binary

Ahoy SAILR! There is No Need to DREAM of C: A Compiler-Aware Structuring Algorithm for Binary Decompilation 361
Zion Leonahenahe Basque, Ati Priya Bajaj, Wil Gibbs, Jude O'Kain, Derron Miao, Tiffany Bao, Adam Doupé, Yan Shoshitaishvili, and Ruoyu Wang, *Arizona State University*

A Taxonomy of C Decompiler Fidelity Issues 379
Luke Dramko and Jeremy Lacomis, *Carnegie Mellon University;* Edward J. Schwartz, *Carnegie Mellon University Software Engineering Institute;* Bogdan Vasilescu and Claire Le Goues, *Carnegie Mellon University*

D-Helix: A Generic Decompiler Testing Framework Using Symbolic Differentiation 397
Muqi Zou, Arslan Khan, Ruoyu Wu, Han Gao, Antonio Bianchi, and Dave (Jing) Tian, *Purdue University*

SymFit: Making the Common (Concrete) Case Fast for Binary-Code Concolic Execution 415
Zhenxiao Qi, Jie Hu, Zhaoqi Xiao, and Heng Yin, *UC Riverside*

Crypto I: Secret Key Exchange

K-Waay: Fast and Deniable Post-Quantum X3DH without Ring Signatures. 433
Daniel Collins and Loïs Huguenin-Dumittan, *EPFL;* Ngoc Khanh Nguyen, *King's College London;* Nicolas Rolin, *Spuerkeess;* Serge Vaudenay, *EPFL*

Diffie-Hellman Picture Show: Key Exchange Stories from Commercial VoWiFi Deployments 451
Gabriel K. Gegenhuber and Florian Holzbauer, *University of Vienna;* Philipp É. Frenzel, *SBA Research;* Edgar Weippl, *University of Vienna and Christian Doppler Laboratory for Security and Quality Improvement in the Production System Lifecycle* (*CDL-SQI*)*;* Adrian Dabrowski, *CISPA Helmholtz Center for Information Security*

Formal verification of the PQXDH Post-Quantum key agreement protocol for end-to-end secure messaging 469
Karthikeyan Bhargavan, *Cryspen;* Charlie Jacomme, *Inria Nancy Grand-Est, Université de Lorraine, LORIA, France;* Franziskus Kiefer, *Cryspen;* Rolfe Schmidt, *Signal Messenger*

Swoosh: Efficient Lattice-Based Non-Interactive Key Exchange 487
Phillip Gajland, *Max Planck Institute for Security and Privacy, Ruhr University Bochum;* Bor de Kock, *NTNU - Norwegian University of Science and Technology, Trondheim, Norway;* Miguel Quaresma, *Max Planck Institute for Security and Privacy;* Giulio Malavolta, *Bocconi University, Max Planck Institute for Security and Privacy;* Peter Schwabe, *Max Planck Institute for Security and Privacy, Radboud University*

Social Issues I: Phishing and Password

PhishDecloaker: Detecting CAPTCHA-cloaked Phishing Websites via Hybrid Vision-based Interactive Models . . . 505
Xiwen Teoh, *Shanghai Jiao Tong University; National University of Singapore;* Yun Lin, *Shanghai Jiao Tong University;* Ruofan Liu, Zhiyong Huang, and Jin Song Dong, *National University of Singapore*

Less Defined Knowledge and More True Alarms: Reference-based Phishing Detection without a Pre-defined Reference List 523
Ruofan Liu, *Shanghai Jiao Tong University/National University of Singapore;* Yun Lin, *Shanghai Jiao Tong University;* Xiwen Teoh, *National University of Singapore;* Gongshen Liu, *Shanghai Jiao Tong University;* Zhiyong Huang and Jin Song Dong, *National University of Singapore*

In Wallet We Trust: Bypassing the Digital Wallets Payment Security for Free Shopping 541
Raja Hasnain Anwar, *University of Massachusetts Amherst;* Syed Rafiul Hussain, *Pennsylvania State University;* Muhammad Taqi Raza, *University of Massachusetts Amherst*

The Impact of Exposed Passwords on Honeyword Efficacy. 559
Zonghao Huang, *Duke University;* Lujo Bauer, *Carnegie Mellon University;* Michael K. Reiter, *Duke University*

Side Channel I: Transient Execution

InSpectre Gadget: Inspecting the Residual Attack Surface of Cross-privilege Spectre v2. 577
Sander Wiebing, Alvise de Faveri Tron, Herbert Bos, and Cristiano Giuffrida, *Vrije Universiteit Amsterdam*

Shesha: Multi-head Microarchitectural Leakage Discovery in new-generation Intel Processors 595
Anirban Chakraborty, Nimish Mishra, and Debdeep Mukhopadhyay, *Indian Institute of Technology Kharagpur*

BeeBox: Hardening BPF against Transient Execution Attacks 613
Di Jin, Alexander J. Gaidis, and Vasileios P. Kemerlis, *Brown University*

SpecLFB: Eliminating Cache Side Channels in Speculative Executions 631
Xiaoyu Cheng, *School of Cyber Science and Engineering, Southeast University, Nanjing, Jiangsu, China; Jiangsu Province Engineering Research Center of Security for Ubiquitous Network, China;* Fei Tong, *School of Cyber Science and Engineering, Southeast University, Nanjing, Jiangsu, China; Jiangsu Province Engineering Research Center of Security for Ubiquitous Network, China; Purple Mountain Laboratories, Nanjing, Jiangsu, China;* Hongyu Wang, *State Key Laboratory of Power Equipment Technology, School of Electrical Engineering, Chongqing University, China; Wiscom System Co., LTD, Nanjing, China;* Zhe Zhou and Fang Jiang, *School of Cyber Science and Engineering, Southeast University, Nanjing, Jiangsu, China; Jiangsu Province Engineering Research Center of Security for Ubiquitous Network, China;* Yuxing Mao, *State Key Laboratory of Power Equipment Technology, School of Electrical Engineering, Chongqing University, China*

Mobile Security I

Towards Privacy-Preserving Social-Media SDKs on Android. 647
Haoran Lu, Yichen Liu, Xiaojing Liao, and Luyi Xing, *Indiana University Bloomington*

UIHash: Detecting Similar Android UIs through Grid-Based Visual Appearance Representation 665
Jiawei Li, *Beihang University; National University of Singapore;* Jian Mao, *Beihang University; Tianmushan Laboratory; Hangzhou Innovation Institute, Beihang University;* Jun Zeng, *National University of Singapore;* Qixiao Lin and Shaowen Feng, *Beihang University;* Zhenkai Liang, *National University of Singapore*

Racing for TLS Certificate Validation: A Hijacker's Guide to the Android TLS Galaxy 683
Sajjad Pourali and Xiufen Yu, *Concordia University;* Lianying Zhao, *Carleton University;* Mohammad Mannan and Amr Youssef, *Concordia University*

DVa: Extracting Victims and Abuse Vectors from Android Accessibility Malware 701
Haichuan Xu, Mingxuan Yao, and Runze Zhang, *Georgia Institute of Technology;* Mohamed Moustafa Dawoud, *German International University;* Jeman Park, *Kyung Hee University;* Brendan Saltaformaggio, *Georgia Institute of Technology*

Web Security I

SoK: State of the Krawlers – Evaluating the Effectiveness of Crawling Algorithms for Web Security Measurements . . .719
Aleksei Stafeev and Giancarlo Pellegrino, *CISPA Helmholtz Center for Information Security*

Vulnerability-oriented Testing for RESTful APIs. 739
Wenlong Du and Jian Li, *School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University;* Yanhao Wang, *Independent Researcher;* Libo Chen, Ruijie Zhao, and Junmin Zhu, *School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University;* Zhengguang Han, *QI-ANXIN Technology Group;* Yijun Wang and Zhi Xue, *School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University*

Web Platform Threats: Automated Detection of Web Security Issues With WPT 757
Pedro Bernardo and Lorenzo Veronese, *TU Wien;* Valentino Dalla Valle and Stefano Calzavara, *Università Ca' Foscari Venezia;* Marco Squarcina, *TU Wien;* Pedro Adão, *Instituto Superior Técnico, Universidade de Lisboa, and Instituto de Telecomunicações;* Matteo Maffei, *TU Wien*

Rise of Inspectron: Automated Black-box Auditing of Cross-platform Electron Apps. 775
Mir Masood Ali, Mohammad Ghasemisharif, Chris Kanich, and Jason Polakis, *University of Illinois Chicago*

LLM for Security

KnowPhish: Large Language Models Meet Multimodal Knowledge Graphs for Enhancing Reference-Based Phishing Detection 793
Yuexin Li, Chengyu Huang, and Shumin Deng, *National University of Singapore;* Mei Lin Lock, *NCS Cyber Special Ops-R&D;* Tri Cao, *National University of Singapore;* Nay Oo and Hoon Wei Lim, *NCS Cyber Special Ops-R&D;* Bryan Hooi, *National University of Singapore*

Exploring ChatGPT's Capabilities on Vulnerability Management 811
Peiyu Liu and Junming Liu, *Zhejiang University NGICS Platform;* Lirong Fu, *Hangzhou Dianzi University;* Kangjie Lu, *University of Minnesota;* Yifan Xia, *Zhejiang University NGICS Platform;* Xuhong Zhang, *Zhejiang University and Jianghuai Advance Technology Center;* Wenzhi Chen, *Zhejiang University;* Haiqin Weng, *Ant Group;* Shouling Ji, *Zhejiang University;* Wenhai Wang, *Zhejiang University NGICS Platform*

Large Language Models for Code Analysis: Do LLMs Really Do Their Job? 829
Chongzhou Fang, Ning Miao, and Shaurya Srivastav, *University of California, Davis;* Jialin Liu, *Temple University;* Ruoyu Zhang, Ruijie Fang, Asmita, Ryan Tsang, and Najmeh Nazari, *University of California, Davis;* Han Wang, *Temple University;* Houman Homayoun, *University of California, Davis*

PentestGPT: Evaluating and Harnessing Large Language Models for Automated Penetration Testing 847
Gelei Deng and Yi Liu, *Nanyang Technological University;* Víctor Mayoral-Vilches, *Alias Robotics and Alpen-Adria-Universität Klagenfurt;* Peng Liu, *Institute for Infocomm Research (I2R), A*STAR, Singapore;* Yuekang Li, *University of New South Wales;* Yuan Xu, Tianwei Zhang, and Yang Liu, *Nanyang Technological University;* Martin Pinzger, *Alpen-Adria-Universität Klagenfurt;* Stefan Rass, *Johannes Kepler University Linz*

Fuzzing I: Software

OptFuzz: Optimization Path Guided Fuzzing for JavaScript JIT Compilers 865
Jiming Wang and Yan Kang, *SKLP, Institute of Computing Technology, CAS & University of Chinese Academy of Sciences;* Chenggang Wu, *SKLP, Institute of Computing Technology, CAS & University of Chinese Academy of Sciences & Zhongguancun Laboratory;* Yuhao Hu, Yue Sun, and Jikai Ren, *SKLP, Institute of Computing Technology, CAS & University of Chinese Academy of Sciences;* Yuanming Lai and Mengyao Xie, *SKLP, Institute of Computing Technology, CAS;* Charles Zhang, *Tsinghua University;* Tao Li, *Nankai University;* Zhe Wang, *SKLP, Institute of Computing Technology, CAS & University of Chinese Academy of Sciences & Zhongguancun Laboratory*

Fuzzing BusyBox: Leveraging LLM and Crash Reuse for Embedded Bug Unearthing 883
Asmita, *University of California, Davis;* Yaroslav Oliinyk and Michael Scott, *NetRise;* Ryan Tsang, Chongzhou Fang, and Houman Homayoun, *University of California, Davis*

Towards Generic Database Management System Fuzzing 901
Yupeng Yang and Yongheng Chen, *Georgia Institute of Technology;* Rui Zhong, *Palo Alto Networks;* Jizhou Chen and Wenke Lee, *Georgia Institute of Technology*

HyperPill: Fuzzing for Hypervisor-bugs by Leveraging the Hardware Virtualization Interface 919
Alexander Bulekov, *EPFL, Boston University, and Amazon;* Qiang Liu, *EPFL and Zhejiang University;* Manuel Egele, *Boston University;* Mathias Payer, *EPFL*

Differential Privacy I

Less is More: Revisiting the Gaussian Mechanism for Differential Privacy 937
Tianxi Ji, *Texas Tech University;* Pan Li, *Case Western Reserve University*

Relation Mining Under Local Differential Privacy 955
Kai Dong, Zheng Zhang, Chuang Jia, Zhen Ling, Ming Yang, and Junzhou Luo, *Southeast University;* Xinwen Fu, *University of Massachusetts Lowell*

Gradients Look Alike: Sensitivity is Often Overestimated in DP-SGD 973
Anvith Thudi and Hengrui Jia, *University of Toronto and Vector Institute;* Casey Meehan, *University of California, San Diego;* Ilia Shumailov, *University of Oxford;* Nicolas Papernot, *University of Toronto and Vector Institute*

DPAdapter: Improving Differentially Private Deep Learning through Noise Tolerance Pre-training 991
Zihao Wang, Rui Zhu, and Dongruo Zhou, *Indiana University Bloomington;* Zhikun Zhang, *Zhejiang University;* John Mitchell, *Stanford University;* Haixu Tang and XiaoFeng Wang, *Indiana University Bloomington*

Deepfake and Synthesis

Double Face: Leveraging User Intelligence to Characterize and Recognize AI-synthesized Faces 1009
Matthew Joslin, Xian Wang, and Shuang Hao, *University of Texas at Dallas*

SoK: The Good, The Bad, and The Unbalanced: Measuring Structural Limitations of Deepfake Media Datasets . . .1027
Seth Layton, Tyler Tucker, Daniel Olszewski, Kevin Warren, Kevin Butler, and Patrick Traynor, *University of Florida*

Can I Hear Your Face? Pervasive Attack on Voice Authentication Systems with a Single Face Image. 1045
Nan Jiang, Bangjie Sun, and Terence Sim, *National University of Singapore;* Jun Han, *KAIST*

dp-promise: Differentially Private Diffusion Probabilistic Models for Image Synthesis 1063
Haichen Wang and Shuchao Pang, *Nanjing University of Science and Technology;* Zhigang Lu, *James Cook University;* Yihang Rao and Yongbin Zhou, *Nanjing University of Science and Technology;* Minhui Xue, *CSIRO's Data61*

Hardware Security II: Architecture and Microarchitecture

DmaAuth: A Lightweight Pointer Integrity-based Secure Architecture to Defeat DMA Attacks 1081
Xingkai Wang, Wenbo Shen, Yujie Bu, Jinmeng Zhou, and Yajin Zhou, *Zhejiang University*

Bending microarchitectural weird machines towards practicality 1099
Ping-Lun Wang, Riccardo Paccagnella, Riad S. Wahby, and Fraser Brown, *Carnegie Mellon University*

GoFetch: Breaking Constant-Time Cryptographic Implementations Using Data Memory-Dependent Prefetchers . . . 1117
Boru Chen, *University of Illinois Urbana-Champaign;* Yingchen Wang, *University of Texas at Austin;* Pradyumna Shome, *Georgia Institute of Technology;* Christopher Fletcher, *University of California, Berkeley;* David Kohlbrenner, *University of Washington;* Riccardo Paccagnella, *Carnegie Mellon University;* Daniel Genkin, *Georgia Institute of Technology*

CacheWarp: Software-based Fault Injection using Selective State Reset 1135
Ruiyi Zhang, Lukas Gerlach, Daniel Weber, and Lorenz Hetterich, *CISPA Helmholtz Center for Information Security;* Youheng Lü, *Independent;* Andreas Kogler, *Graz University of Technology;* Michael Schwarz, *CISPA Helmholtz Center for Information Security*

System Security II: OS Kernel

Moat: Towards Safe BPF Kernel Extension 1153
Hongyi Lu, *Research Institute of Trustworthy Autonomous Systems, Southern University of Science and Technology, and Hong Kong University of Science and Technology;* Shuai Wang, *Hong Kong University of Science and Technology;* Yechang Wu and Wanning He, *Southern University of Science and Technology;* Fengwei Zhang, *Southern University of Science and Technology and Research Institute of Trustworthy Autonomous Systems*

SeaK: Rethinking the Design of a Secure Allocator for OS Kernel 1171
Zicheng Wang, *University of Colorado Boulder & Nanjing University;* Yicheng Guang, *Nanjing University;* Yueqi Chen, *University of Colorado Boulder;* Zhenpeng Lin, *Northwestern University;* Michael Le, *IBM Research;* Dang K Le, *Northwestern University;* Dan Williams, *Virginia Tech;* Xinyu Xing, *Northwestern University;* Zhongshu Gu and Hani Jamjoom, *IBM Research*

Take a Step Further: Understanding Page Spray in Linux Kernel Exploitation 1189
Ziyi Guo, Dang K Le, and Zhenpeng Lin, *Northwestern University;* Kyle Zeng, Ruoyu Wang, Tiffany Bao, Yan Shoshitaishvili, and Adam Doupé, *Arizona State University;* Xinyu Xing, *Northwestern University*

SafeFetch: Practical Double-Fetch Protection with Kernel-Fetch Caching 1207
Victor Duta, Mitchel Josephus Aloserij, and Cristiano Giuffrida, *Vrije Universiteit Amsterdam*

Network Security II: Attacks

LanDscAPe: Exploring LDAP Weaknesses and Data Leaks at Internet Scale 1225
Jonas Kaspereit and Gurur Öndarö, *Münster University of Applied Sciences;* Gustavo Luvizotto Cesar, *University of Twente;* Simon Ebbers, *Münster University of Applied Sciences;* Fabian Ising, *Fraunhofer SIT and National Research Center for Applied Cybersecurity ATHENE;* Christoph Saatjohann, *Münster University of Applied Sciences, Fraunhofer SIT, and National Research Center for Applied Cybersecurity ATHENE;* Mattijs Jonker, *University of Twente;* Ralph Holz, *University of Twente and University of Münster;* Sebastian Schinzel, *Münster University of Applied Sciences, Fraunhofer SIT, and National Research Center for Applied Cybersecurity ATHENE*

FakeBehalf: Imperceptible Email Spoofing Attacks against the Delegation Mechanism in Email Systems. 1243
Jinrui Ma, Lutong Chen, and Kaiping Xue, *University of Science and Technology of China;* Bo Luo, *The University of Kansas;* Xuanbo Huang, Mingrui Ai, and Huanjie Zhang, *University of Science and Technology of China;* David S.L. Wei, *Fordham University;* Yan Zhuang, *University of Science and Technology of China*

Rethinking the Security Threats of Stale DNS Glue Records 1261
Yunyi Zhang, *National University of Defense Technology and Tsinghua University;* Baojun Liu, *Tsinghua University;* Haixin Duan, *Tsinghua University, Zhongguancun Laboratory, and Quan Cheng Laboratory;* Min Zhang, *National University of Defense Technology;* Xiang Li, *Tsinghua University;* Fan Shi and Chengxi Xu, *National University of Defense Technology;* Eihal Alowaisheq, *King Saud University*

EVOKE: Efficient Revocation of Verifiable Credentials in IoT Networks 1279
Carlo Mazzocca, *University of Bologna;* Abbas Acar and Selcuk Uluagac, *Cyber-Physical Systems Security Lab, Florida International University;* Rebecca Montanari, *University of Bologna*

ML II: Fault Injection and Robustness

DNN-GP: Diagnosing and Mitigating Model's Faults Using Latent Concepts 1297
Shuo Wang, *Shanghai Jiao Tong University;* Hongsheng Hu, *CSIRO's Data61;* Jiamin Chang, *University of New South Wales and CSIRO's Data61;* Benjamin Zi Hao Zhao, *Macquarie University;* Qi Alfred Chen, *University of California, Irvine;* Minhui Xue, *CSIRO's Data61*

Yes, One-Bit-Flip Matters! Universal DNN Model Inference Depletion with Runtime Code Fault Injection 1315
Shaofeng Li, *Peng Cheng Laboratory;* Xinyu Wang, *Shanghai Jiao Tong University;* Minhui Xue, *CSIRO's Data61;* Haojin Zhu, *Shanghai Jiao Tong University;* Zhi Zhang, *University of Western Australia;* Yansong Gao, *CSIRO's Data61;* Wen Wu, *Peng Cheng Laboratory;* Xuemin (Sherman) Shen, *University of Waterloo*

Tossing in the Dark: Practical Bit-Flipping on Gray-box Deep Neural Networks for Runtime Trojan Injection . . 1331
Zihao Wang, Di Tang, and XiaoFeng Wang, *Indiana University Bloomington;* Wei He, Zhaoyang Geng, and Wenhao Wang, *SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences*

Forget and Rewire: Enhancing the Resilience of Transformer-based Models against Bit-Flip Attacks 1349
Najmeh Nazari, Hosein Mohammadi Makrani, and Chongzhou Fang, *University of California, Davis;* Hossein Sayadi, *California State University, Long Beach;* Setareh Rafatirad, *University of California, Davis;* Khaled N. Khasawneh, *George Mason University;* Houman Homayoun, *University of California, Davis*

Security Analysis II: Program Analysis

What IF Is Not Enough? Fixing Null Pointer Dereference With Contextual Check 1367
Yunlong Xing, Shu Wang, Shiyu Sun, Xu He, and Kun Sun, *George Mason University;* Qi Li, *Tsinghua University*

Unleashing the Power of Type-Based Call Graph Construction by Using Regional Pointer Information 1383
Yuandao Cai, Yibo Jin, and Charles Zhang, *The Hong Kong University of Science and Technology*

Practical Data-Only Attack Generation 1401
Brian Johannesmeyer, Asia Slowinska, Herbert Bos, and Cristiano Giuffrida, *Vrije Universiteit Amsterdam*

Don't Waste My Efforts: Pruning Redundant Sanitizer Checks by Developer-Implemented Type Checks 1419
Yizhuo Zhai, Zhiyun Qian, Chengyu Song, Manu Sridharan, and Trent Jaeger, *University of California, Riverside;* Paul Yu, *U.S. Army Research Laboratory;* Srikanth V. Krishnamurthy, *University of California, Riverside*

Zero-Knowledge Proof I

Two Shuffles Make a RAM: Improved Constant Overhead Zero Knowledge RAM. 1435
Yibin Yang, *Georgia Institute of Technology;* David Heath, *University of Illinois Urbana-Champaign*

Notus: Dynamic Proofs of Liabilities from Zero-knowledge RSA Accumulators 1453
Jiajun Xin, Arman Haghighi, Xiangan Tian, and Dimitrios Papadopoulos, *The Hong Kong University of Science and Technology*

Practical Security Analysis of Zero-Knowledge Proof Circuits. 1471
Hongbo Wen, *University of California, Santa Barbara;* Jon Stephens, *The University of Texas at Austin and Veridise;* Yanju Chen, *University of California, Santa Barbara;* Kostas Ferles, *Veridise;* Shankara Pailoor, *The University of Texas at Austin and Veridise;* Kyle Charbonnet, *Ethereum Foundation;* Isil Dillig, *The University of Texas at Austin and Veridise;* Yu Feng, *University of California, Santa Barbara, and Veridise*

Formalizing Soundness Proofs of Linear PCP SNARKs 1489
Bolton Bailey and Andrew Miller, *University of Illinois at Urbana-Champaign*

Measurement I: Fraud and Malware and Spam

Guardians of the Galaxy: Content Moderation in the InterPlanetary File System 1507
Saidu Sokoto, *City, University of London;* Leonhard Balduf, *TU Darmstadt;* Dennis Trautwein, *University of Göttingen;* Yiluo Wei and Gareth Tyson, *Hong Kong Univ. of Science & Technology (GZ);* Ignacio Castro, *Queen Mary, University of London;* Onur Ascigil, *Lancaster University;* George Pavlou, *University College London;* Maciej Korczyński, *Univ. Grenoble Alpes;* Björn Scheuermann, *TU Darmstadt;* Michał Król, *City, University of London*

True Attacks, Attack Attempts, or Benign Triggers? An Empirical Measurement of Network Alerts in a Security Operations Center 1525
Limin Yang, Zhi Chen, Chenkai Wang, Zhenning Zhang, and Sushruth Booma, *University of Illinois at Urbana-Champaign;* Phuong Cao, *NCSA;* Constantin Adam, *IBM Research;* Alexander Withers, *NCSA;* Zbigniew Kalbarczyk, Ravishankar K. Iyer, and Gang Wang, *University of Illinois at Urbana-Champaign*

DarkFleece: Probing the Dark Side of Android Subscription Apps 1543
Chang Yue, *Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China;* Chen Zhong, *University of Tampa, USA;* Kai Chen and Zhiyu Zhang, *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*

Into the Dark: Unveiling Internal Site Search Abused for Black Hat SEO 1561
Yunyi Zhang, *National University of Defense Technology; Tsinghua University;* Mingxuan Liu, *Zhongguancun Laboratory;* Baojun Liu, *Tsinghua University; Zhongguancun Laboratory;* Yiming Zhang, *Tsinghua University;* Haixin Duan, *Tsinghua University; Zhongguancun Laboratory;* Min Zhang, *National University of Defense Technology;* Hui Jiang, *Tsinghua University; Baidu Inc;* Yanzhe Li, *Baidu Inc;* Fan Shi, *National University of Defense Technology*

Side Channel II: RowHammer

ABACuS: All-Bank Activation Counters for Scalable and Low Overhead RowHammer Mitigation 1579
Ataberk Olgun, Yahya Can Tugrul, Nisa Bostanci, Ismail Emir Yuksel, Haocong Luo, Steve Rhyner, Abdullah Giray Yaglikci, Geraldo F. Oliveira, and Onur Mutlu, *ETH Zurich*

SledgeHammer: Amplifying Rowhammer via Bank-level Parallelism 1597
Ingab Kang, *University of Michigan;* Walter Wang and Jason Kim, *Georgia Tech;* Stephan van Schaik and Youssef Tobah, *University of Michigan;* Daniel Genkin, *Georgia Tech;* Andrew Kwong, *UNC Chapel Hill;* Yuval Yarom, *Ruhr University Bochum*

ZenHammer: Rowhammer Attacks on AMD Zen-based Platforms 1615
Patrick Jattke, Max Wipfli, Flavien Solt, Michele Marazzi, Matej Bölcskei, and Kaveh Razavi, *ETH Zurich*

Go Go Gadget Hammer: Flipping Nested Pointers for Arbitrary Data Leakage 1635
Youssef Tobah, *University of Michigan;* Andrew Kwong, *UNC Chapel Hill;* Ingab Kang, *University of Michigan;* Daniel Genkin, *Georgia Tech;* Kang G. Shin, *University of Michigan*

Forensics

00SEVen – Re-enabling Virtual Machine Forensics: Introspecting Confidential VMs Using Privileged in-VM Agents. 1651
Fabian Schwarz and Christian Rossow, *CISPA Helmholtz Center for Information Security*

WebRR: A Forensic System for Replaying and Investigating Web-Based Attacks in The Modern Web 1669
Joey Allen, *Palo Alto Networks;* Zheng Yang, Feng Xiao, and Matthew Landen, *Georgia Institute of Technology;* Roberto Perdisci, *Georgia Institute of Technology and University of Georgia;* Wenke Lee, *Georgia Institute of Technology*

AI Psychiatry: Forensic Investigation of Deep Learning Networks in Memory Images 1687
David Oygenblik, *Georgia Institute of Technology;* Carter Yagemann, *Ohio State University;* Joseph Zhang, *University of Pennsylvania;* Arianna Mastali, *Georgia Institute of Technology;* Jeman Park, *Kyung Hee University;* Brendan Saltaformaggio, *Georgia Institute of Technology*

Cost-effective Attack Forensics by Recording and Correlating File System Changes. 1705
Le Yu, Yapeng Ye, Zhuo Zhang, and Xiangyu Zhang, *Purdue University*

ML for Security

Automated Large-Scale Analysis of Cookie Notice Compliance 1723
Ahmed Bouhoula, Karel Kubicek, Amit Zac, Carlos Cotrini, and David Basin, *ETH Zurich*

Detecting and Mitigating Sampling Bias in Cybersecurity with Unlabeled Data 1741
Saravanan Thirumuruganathan, *Independent Researcher;* Fatih Deniz, Issa Khalil, and Ting Yu, *Qatar Computing Research Institute, HBKU;* Mohamed Nabeel, *Palo Alto Networks;* Mourad Ouzzani, *Qatar Computing Research Institute, HBKU*

Code is not Natural Language: Unlock the Power of Semantics-Oriented Graph Representation for Binary Code Similarity Detection 1759
Haojie He, *School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University;* Xingwei Lin, *Ant Group;* Ziang Weng and Ruijie Zhao, *School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University;* Shuitao Gan, *Laboratory for Advanced Computing and Intelligence Engineering;* Libo Chen, *School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University;* Yuede Ji, *University of North Texas;* Jiashui Wang, *Ant Group;* Zhi Xue, *School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University*

VulSim: Leveraging Similarity of Multi-Dimensional Neighbor Embeddings for Vulnerability Detection 1777
Samiha Shimmi, Ashiqur Rahman, and Mohan Gadde, *Northern Illinois University;* Hamed Okhravi, *MIT Lincoln Laboratory;* Mona Rahimi, *Northern Illinois University*

LLM I: Attack and Defense

An LLM-Assisted Easy-to-Trigger Backdoor Attack on Code Completion Models: Injecting Disguised Vulnerabilities against Strong Detection 1795
Shenao Yan, *University of Connecticut;* Shen Wang and Yue Duan, *Singapore Management University;* Hanbin Hong, *University of Connecticut;* Kiho Lee and Doowon Kim, *University of Tennessee, Knoxville;* Yuan Hong, *University of Connecticut*

REMARK-LLM: A *R*obust and *E*fficient Water*mark*ing Framework for Generative Large Language Models 1813
Ruisi Zhang, Shehzeen Samarah Hussain, Paarth Neekhara, and Farinaz Koushanfar, *University of California, San Diego*

Formalizing and Benchmarking Prompt Injection Attacks and Defenses 1831
Yupei Liu, *The Pennsylvania State University;* Yuqi Jia, *Duke University;* Runpeng Geng and Jinyuan Jia, *The Pennsylvania State University;* Neil Zhenqiang Gong, *Duke University*

Instruction Backdoor Attacks Against Customized LLMs 1849
Rui Zhang and Hongwei Li, *University of Electronic Science and Technology of China;* Rui Wen, *CISPA Helmholtz Center for Information Security;* Wenbo Jiang and Yuan Zhang, *University of Electronic Science and Technology of China;* Michael Backes, *CISPA Helmholtz Center for Information Security;* Yun Shen, *NetApp;* Yang Zhang, *CISPA Helmholtz Center for Information Security*

Software Vulnerability Detection

FIRE: Combining Multi-Stage Filtering with Taint Analysis for Scalable Recurring Vulnerability Detection . . . 1867
Siyue Feng, *National Engineering Research Center for Big Data Technology and System, Services Computing Technology and System Lab, Hubei Key Laboratory of Distributed System Security, Hubei Engineering Research Center on Big Data Security, Cluster and Grid Computing Lab; School of Cyber Science and Engineering, Huazhong University of Science and Technology;* Yueming Wu, *Nanyang Technological University;* Wenjie Xue and Sikui Pan, *National Engineering Research Center for Big Data Technology and System, Services Computing Technology and System Lab, Hubei Key Laboratory of Distributed System Security, Hubei Engineering Research Center on Big Data Security, Cluster and Grid Computing Lab; School of Cyber Science and Engineering, Huazhong University of Science and Technology;* Deqing Zou, *National Engineering Research Center for Big Data Technology and System, Services Computing Technology and System Lab, Hubei Key Laboratory of Distributed System Security, Hubei Engineering Research Center on Big Data Security, Cluster and Grid Computing Lab; School of Cyber Science and Engineering, Huazhong University of Science and Technology; Jinyinhu Laboratory;* Yang Liu, *Nanyang Technological University;* Hai Jin, *National Engineering Research Center for Big Data Technology and System, Services Computing Technology and System Lab, Hubei Key Laboratory of Distributed System Security, Hubei Engineering Research Center on Big Data Security, Cluster and Grid Computing Lab; School of Computer Science and Technology, Huazhong University of Science and Technology*

Inference of Error Specifications and Bug Detection Using Structural Similarities 1885
Nora Dossche and Bart Coppens, *Ghent University*

A Binary-level Thread Sanitizer or *Why Sanitizing on the Binary Level is Hard* 1903
Joschua Schilling, *CISPA Helmholtz Center for Information Security;* Andreas Wendler, *Friedrich-Alexander-Universität Erlangen-Nürnberg;* Philipp Görz, Nils Bars, Moritz Schloegel, and Thorsten Holz, *CISPA Helmholtz Center for Information Security*

ORANalyst: Systematic Testing Framework for Open RAN Implementations 1921
Tianchang Yang, Syed Md Mukit Rashid, Ali Ranjbar, Gang Tan, and Syed Rafiul Hussain, *The Pennsylvania State University*

Cryptographic Protocols I: Multi-Party Computation

Scalable Multi-Party Computation Protocols for Machine Learning in the Honest-Majority Setting 1939
Fengrun Liu, *University of Science and Technology of China & Shanghai Qi Zhi Institute;* Xiang Xie, *Shanghai Qi Zhi Institute & PADO Labs;* Yu Yu, *Shanghai Jiao Tong University & State Key Laboratory of Cryptology*

Lightweight Authentication of Web Data via Garble-Then-Prove 1957
Xiang Xie, *PADO Labs;* Kang Yang, *State Key Laboratory of Cryptology;* Xiao Wang, *Northwestern University;* Yu Yu, *Shanghai Jiao Tong University and Shanghai Qi Zhi Institute*

Holding Secrets Accountable: Auditing Privacy-Preserving Machine Learning 1975
Hidde Lycklama, *ETH Zurich;* Alexander Viand, *Intel Labs;* Nicolas Küchler, *ETH Zurich;* Christian Knabenhans, *EPFL;* Anwar Hithnawi, *ETH Zurich*

Secure Account Recovery for a Privacy-Preserving Web Service 1993
Ryan Little, *Boston University;* Lucy Qin, *Georgetown University;* Mayank Varia, *Boston University*

Thursday, August 15

User Studies II: At-Risk Users

Navigating Traumatic Stress Reactions During Computer Security Interventions 2011
Lana Ramjit, *Cornell Tech;* Natalie Dolci, *UW-Safe Campus;* Francesca Rossi, *Thriving Through;* Ryan Garcia, *UW-Safe Campus;* Thomas Ristenpart, *Cornell Tech;* Dana Cuomo, *Lafayette College*

Exploring digital security and privacy in relative poverty in Germany through qualitative interviews 2029
Anastassija Kostan and Sara Olschar, *Paderborn University;* Lucy Simko, *The George Washington University;* Yasemin Acar, *Paderborn University & The George Washington University*

"But they have overlooked a few things in Afghanistan:" An Analysis of the Integration of Biometric Voter Verification in the 2019 Afghan Presidential Elections 2047
Kabir Panahi and Shawn Robertson, *University of Kansas;* Yasemin Acar, *Paderborn University;* Alexandru G. Bardas, *University of Kansas;* Tadayoshi Kohno, *University of Washington;* Lucy Simko, *The George Washington University*

Understanding How to Inform Blind and Low-Vision Users about Data Privacy through Privacy Question Answering Assistants 2065
Yuanyuan Feng, *University of Vermont;* Abhilasha Ravichander, *Allen Institute for Artificial Intelligence;* Yaxing Yao, *Virginia Tech;* Shikun Zhang and Rex Chen, *Carnegie Mellon University;* Shomir Wilson, *Pennsylvania State University;* Norman Sadeh, *Carnegie Mellon University*

Assessing Suspicious Emails with Banner Warnings Among Blind and Low-Vision Users in Realistic Settings . . . 2083
Filipo Sharevski, *DePaul University;* Aziz Zeidieh, *University of Illinois at Urbana-Champaign*

Side Channel III

INVALIDATE+COMPARE: A Timer-Free GPU Cache Attack Primitive 2101
Zhenkai Zhang, *Clemson University;* Kunbei Cai, *University of Central Florida;* Yanan Guo, *University of Rochester;* Fan Yao, *University of Central Florida;* Xing Gao, *University of Delaware*

Peep With A Mirror: Breaking The Integrity of Android App Sandboxing via Unprivileged Cache Side Channel . . . 2119
Yan Lin, *Jinan University;* Joshua Wong, *Singapore Management University;* Xiang Li and Haoyu Ma, *Zhejiang Lab;* Debin Gao, *Singapore Management University*

Indirector: High-Precision Branch Target Injection Attacks Exploiting the Indirect Branch Predictor 2137
Luyi Li, Hosein Yavarzadeh, and Dean Tullsen, *UC San Diego*

Intellectual Property Exposure: Subverting and Securing Intellectual Property Encapsulation in Texas Instruments Microcontrollers 2155
Marton Bognar, Cas Magnus, Frank Piessens, and Jo Van Bulck, *DistriNet, KU Leuven*

ML III: Secure ML

AutoFHE: Automated Adaption of CNNs for Efficient Evaluation over FHE 2173
Wei Ao and Vishnu Naresh Boddeti, *Michigan State University*

Fast and Private Inference of Deep Neural Networks by Co-designing Activation Functions 2191
Abdulrahman Diaa, Lucas Fenaux, Thomas Humphries, Marian Dietz, Faezeh Ebrahimianghazani, Bailey Kacsmar, Xinda Li, Nils Lukas, Rasoul Akhavan Mahdavi, and Simon Oya, *University of Waterloo;* Ehsan Amjadian, *University of Waterloo and Royal Bank of Canada;* Florian Kerschbaum, *University of Waterloo*

OblivGNN: Oblivious Inference on Transductive and Inductive Graph Neural Network 2209
Zhibo Xu, *Monash University and CSIRO's Data61;* Shangqi Lai, *CSIRO's Data61;* Xiaoning Liu, *RMIT University;* Alsharif Abuadbba, *CSIRO's Data61;* Xingliang Yuan, *The University of Melbourne;* Xun Yi, *RMIT University*

MD-ML: Super Fast Privacy-Preserving Machine Learning for Malicious Security with a Dishonest Majority . . . 2227
Boshi Yuan, Shixuan Yang, and Yongxiang Zhang, *Shanghai Jiao Tong University, China;* Ning Ding, Dawu Gu, and Shi-Feng Sun, *Shanghai Jiao Tong University, China; Shanghai Jiao Tong University* (*Wuxi*) *Blockchain Advanced Research Center*

Accelerating Secure Collaborative Machine Learning with Protocol-Aware RDMA 2245
Zhenghang Ren, Mingxuan Fan, Zilong Wang, Junxue Zhang, and Chaoliang Zeng, *iSING Lab@The Hong Kong University of Science and Technology;* Zhicong Huang and Cheng Hong, *Ant Group;* Kai Chen, *iSING Lab@The Hong Kong University of Science and Technology and University of Science and Technology of China*

Measurement II: Network

CalcuLatency: Leveraging Cross-Layer Network Latency Measurements to Detect Proxy-Enabled Abuse 2263
Reethika Ramesh, *University of Michigan;* Philipp Winter, *Independent;* Sam Korman and Roya Ensafi, *University of Michigan*

6Sense: Internet-Wide IPv6 Scanning and its Security Applications 2281
Grant Williams, Mert Erdemir, Amanda Hsu, Shraddha Bhat, Abhishek Bhaskar, Frank Li, and Paul Pearce, *Georgia Institute of Technology*

A Flushing Attack on the DNS Cache 2299
Yehuda Afek and Anat Bremler-Barr, *Tel-Aviv University;* Shoham Danino, *Reichman University;* Yuval Shavitt, *Tel-Aviv University*

SnailLoad: Exploiting Remote Network Latency Measurements without JavaScript 2315
Stefan Gast, Roland Czerny, Jonas Juffinger, Fabian Rauscher, Simone Franza, and Daniel Gruss, *Graz University of Technology*

An Interview Study on Third-Party Cyber Threat Hunting Processes in the U.S. Department of Homeland Security 2333
William P. Maxam III, *US Coast Guard Academy;* James C. Davis, *Purdue University*

ML IV: Privacy Inference I

A Linear Reconstruction Approach for Attribute Inference Attacks against Synthetic Data 2351
Meenatchi Sundaram Muthu Selva Annamalai, *University College London;* Andrea Gadotti and Luc Rocher, *University of Oxford*

Did the Neurons Read your Book? Document-level Membership Inference for Large Language Models 2369
Matthieu Meeus, *Imperial College London;* Shubham Jain, *Sense Street;* Marek Rei and Yves-Alexandre de Montjoye, *Imperial College London*

MIST: Defending Against Membership Inference Attacks Through Membership-Invariant Subspace Training . . . 2387
Jiacheng Li, Ninghui Li, and Bruno Ribeiro, *Purdue University*

Inf^{2}Guard: An Information-Theoretic Framework for Learning Privacy-Preserving Representations against Inference Attacks 2405
Sayedeh Leila Noorbakhsh and Binghui Zhang, *Illinois Institute of Technology;* Yuan Hong, *University of Connecticut;* Binghui Wang, *Illinois Institute of Technology*

Property Existence Inference against Generative Models 2423
Lijin Wang, Jingjing Wang, Jie Wan, and Lin Long, *Zhejiang University;* Ziqi Yang and Zhan Qin, *Zhejiang University, ZJU-Hangzhou Global Scientific and Technological Innovation Center*

Fuzzing II: Method

SDFuzz: Target States Driven Directed Fuzzing 2441
Penghui Li, *The Chinese University of Hong Kong and Zhongguancun Laboratory;* Wei Meng, *The Chinese University of Hong Kong;* Chao Zhang, *Tsinghua University and Zhongguancun Laboratory*

Critical Code Guided Directed Greybox Fuzzing for Commits 2459
Yi Xiang, *Zhejiang University NGICS Platform;* Xuhong Zhang, *Zhejiang University and Jianghuai Advance Technology Center;* Peiyu Liu, *Zhejiang University NGICS Platform;* Shouling Ji, Xiao Xiao, Hong Liang, and Jiacheng Xu, *Zhejiang University;* Wenhai Wang, *Zhejiang University NGICS Platform*

Toward Unbiased Multiple-Target Fuzzing with Path Diversity 2475
Huanyao Rong, *Indiana University Bloomington;* Wei You, *Renmin University of China;* XiaoFeng Wang and Tianhao Mao, *Indiana University Bloomington*

SymBisect: Accurate Bisection for Fuzzer-Exposed Vulnerabilities 2493
Zheng Zhang and Yu Hao, *UC Riverside;* Weiteng Chen, *Microsoft Research;* Xiaochen Zou, Xingyu Li, Haonan Li, Yizhuo Zhai, and Zhiyun Qian, *UC Riverside;* Billy Lau, *Google*

Data Coverage for Guided Fuzzing 2511
Mingzhe Wang, Jie Liang, Chijin Zhou, Zhiyong Wu, Jingzhou Fu, and Zhuo Su, *Tsinghua University;* Qing Liao, *Harbin Institute of Technology;* Bin Gu, *Beijing Institute of Control Engineering;* Bodong Wu, *Huawei Technologies Co., Ltd;* Yu Jiang, *Tsinghua University*

Crypto II: Searchable Encryption

I/O-Efficient Dynamic Searchable Encryption meets Forward & Backward Privacy 2527
Priyanka Mondal, *University of California, Santa Cruz;* Javad Ghareh Chamani, *HKUST;* Ioannis Demertzis, *University of California, Santa Cruz;* Dimitrios Papadopoulos, *HKUST*

FEASE: Fast and Expressive Asymmetric Searchable Encryption 2545
Long Meng, Liqun Chen, and Yangguang Tian, *University of Surrey;* Mark Manulis, *Universität der Bundeswehr München;* Suhui Liu, *Southeast University*

***d*-DSE: Distinct Dynamic Searchable Encryption Resisting Volume Leakage in Encrypted Databases. 2563**
Dongli Liu and Wei Wang, *Huazhong University of Science and Technology;* Peng Xu, *Huazhong University of Science and Technology, Hubei Key Laboratory of Distributed System Security, School of Cyber Science and Engineering, JinYinHu Laboratory, and State Key Laboratory of Cryptology;* Laurence T. Yang, *Huazhong University of Science and Technology and St. Francis Xavier University;* Bo Luo, *The University of Kansas;* Kaitai Liang, *Delft University of Technology*

MUSES: Efficient Multi-User Searchable Encrypted Database 2581
Tung Le, *Virginia Tech;* Rouzbeh Behnia, *University of South Florida;* Jorge Guajardo, *Robert Bosch Research and Technology Center;* Thang Hoang, *Virginia Tech*

Query Recovery from Easy to Hard: Jigsaw Attack against SSE 2599
Hao Nie and Wei Wang, *Huazhong University of Science and Technology;* Peng Xu, *Huazhong University of Science and Technology, Hubei Key Laboratory of Distributed System Security, School of Cyber Science and Engineering, JinYinHu Laboratory, and State Key Laboratory of Cryptology;* Xianglong Zhang, *Huazhong University of Science and Technology;* Laurence T. Yang, *Huazhong University of Science and Technology and St. Francis Xavier University;* Kaitai Liang, *Delft University of Technology*

Social Issues II: Surveillance and Censorship

GFWeb: Measuring the Great Firewall's Web Censorship at Scale 2617
Nguyen Phong Hoang, *University of British Columbia and University of Chicago;* Jakub Dalek and Masashi Crete-Nishihata, *Citizen Lab - University of Toronto;* Nicolas Christin, *Carnegie Mellon University;* Vinod Yegneswaran, *SRI International;* Michalis Polychronakis, *Stony Brook University;* Nick Feamster, *University of Chicago*

Snowflake, a censorship circumvention system using temporary WebRTC proxies 2635
Cecylia Bocovich, *Tor Project;* Arlo Breault, *Wikimedia Foundation;* David Fifield and Serene, *unaffiliated;* Xiaokang Wang, *Tor Project*

SpotProxy: Rediscovering the Cloud for Censorship Circumvention 2653
Patrick Tser Jern Kon, *University of Michigan;* Sina Kamali, *University of Waterloo;* Jinyu Pei, *Rice University;* Diogo Barradas, *University of Waterloo;* Ang Chen, *University of Michigan;* Micah Sherr, *Georgetown University;* Moti Yung, *Google and Columbia University*

Bridging Barriers: A Survey of Challenges and Priorities in the Censorship Circumvention Landscape 2671
Diwen Xue, Anna Ablove, and Reethika Ramesh, *University of Michigan;* Grace Kwak Danciu, *Independent;* Roya Ensafi, *University of Michigan*

Fingerprinting Obfuscated Proxy Traffic with Encapsulated TLS Handshakes 2689
Diwen Xue, *University of Michigan;* Michalis Kallitsis, *Merit Network, Inc.;* Amir Houmansadr, *UMass Amherst;* Roya Ensafi, *University of Michigan*

AR and VR

When the User Is Inside the User Interface: An Empirical Study of UI Security Properties in Augmented Reality. . 2707
Kaiming Cheng, Arkaprabha Bhattacharya, Michelle Lin, Jaewook Lee, Aroosh Kumar, Jeffery F. Tian, Tadayoshi Kohno, and Franziska Roesner, *University of Washington*

Can Virtual Reality Protect Users from Keystroke Inference Attacks? 2725
Zhuolin Yang, Zain Sarwar, Iris Hwang, Ronik Bhaskar, Ben Y. Zhao, and Haitao Zheng, *University of Chicago*

Remote Keylogging Attacks in Multi-user VR Applications 2743
Zihao Su, *University of California, Santa Barbara;* Kunlin Cai, *University of California, Los Angeles;* Reuben Beeler, Lukas Dresel, Allan Garcia, and Ilya Grishchenko, *University of California, Santa Barbara;* Yuan Tian, *University of California, Los Angeles;* Christopher Kruegel and Giovanni Vigna, *University of California, Santa Barbara*

That Doesn't Go There: Attacks on Shared State in Multi-User Augmented Reality Applications 2761
Carter Slocum, Yicheng Zhang, Erfan Shayegani, Pedram Zaree, and Nael Abu-Ghazaleh, *University of California, Riverside;* Jiasi Chen, *University of Michigan*

Penetration Vision through Virtual Reality Headsets: Identifying 360-degree Videos from Head Movements. . . . 2779
Anh Nguyen, Xiaokuan Zhang, and Zhisheng Yan, *George Mason University*

User Studies III: Privacy I

"I'm not convinced that they don't collect more than is necessary": User-Controlled Data Minimization Design in Search Engines 2797
Tanusree Sharma, *University of Illinois at Urbana-Champaign;* Lin Kyi, *Max Planck Institute for Security and Privacy;* Yang Wang, *University of Illinois at Urbana-Champaign;* Asia J. Biega, *Max Planck Institute for Security and Privacy*

The Effect of Design Patterns on (Present and Future) Cookie Consent Decisions. 2813
Nataliia Bielova, *Inria research centre at Université Côte d'Azur;* Laura Litvine and Anysia Nguyen, *Behavioural Insights Team* (*BIT*)*;* Mariam Chammat, *Interministerial Directorate for Public Transformation* (*DITP*)*;* Vincent Toubiana, *Commission Nationale de l'Informatique et des Libertés* (*CNIL*)*;* Estelle Hary, *RMIT University*

Unpacking Privacy Labels: A Measurement and Developer Perspective on Google's Data Safety Section 2831
Rishabh Khandelwal, Asmit Nayak, Paul Chung, and Kassem Fawaz, *University of Wisconsin-Madison*

Dissecting Privacy Perspectives of Websites Around the World: "Aceptar Todo, Alle Akzeptieren, Accept All..." . . . 2849
Aysun Ogut, Berke Turanlioglu, Doruk Can Metiner, Albert Levi, Cemal Yilmaz, and Orcun Cetin, *Sabanci University, Tuzla, Istanbul, Turkiye;* Selcuk Uluagac, *Cyber-Physical Systems Security Lab, Florida International University, Miami, Florida, USA*

Data Subjects' Reactions to Exercising Their Right of Access. 2865
Arthur Borem, Elleen Pan, Olufunmilola Obielodan, Aurelie Roubinowitz, and Luca Dovichi, *University of Chicago;* Michelle L. Mazurek, *University of Maryland;* Blase Ur, *University of Chicago*

ML V: Backdoor Defense

Neural Network Semantic Backdoor Detection and Mitigation: A Causality-Based Approach. 2883
Bing Sun, Jun Sun, and Wayne Koh, *Singapore Management University;* Jie Shi, *Huawei Singapore*

On the Difficulty of Defending Contrastive Learning against Backdoor Attacks 2901
Changjiang Li, *Stony Brook University;* Ren Pang, Bochuan Cao, Zhaohan Xi, and Jinghui Chen, *Pennsylvania State University;* Shouling Ji, *Zhejiang University;* Ting Wang, *Stony Brook University*

Mudjacking: Patching Backdoor Vulnerabilities in Foundation Models 2919
Hongbin Liu, Michael K. Reiter, and Neil Zhenqiang Gong, *Duke University*

Xplain: Analyzing Invisible Correlations in Model Explanation 2937
Kavita Kumari and Alessandro Pegoraro, *Technical University of Darmstadt;* Hossein Fereidooni, *Kobil;* Ahmad-Reza Sadeghi, *Technical University of Darmstadt*

Verify your Labels! Trustworthy Predictions and Datasets via Confidence Scores 2955
Torsten Krauß, Jasper Stang, and Alexandra Dmitrienko, *University of Würzburg*

ML VI: Digital Adversarial Attacks

More Simplicity for Trainers, More Opportunity for Attackers: Black-Box Attacks on Speaker Recognition Systems by Inferring Feature Extractor 2973
Yunjie Ge, Pinji Chen, Qian Wang, Lingchen Zhao, and Ningping Mou, *Wuhan University;* Peipei Jiang, *Wuhan University; City University of Hong Kong;* Cong Wang, *City University of Hong Kong;* Qi Li, *Tsinghua University;* Chao Shen, *Xi'an Jiaotong University*

Transferability of White-box Perturbations: Query-Efficient Adversarial Attacks against Commercial DNN Services 2991
Meng Shen and Changyue Li, *School of Cyberspace Science and Technology, Beijing Institute of Technology, China;* Qi Li, *Institute for Network Sciences and Cyberspace, Tsinghua University, China;* Hao Lu, *School of Computer Science and Technology, Beijing Institute of Technology, China;* Liehuang Zhu, *School of Cyberspace Science and Technology, Beijing Institute of Technology, China;* Ke Xu, *Department of Computer Science, Tsinghua University, China*

Adversarial Illusions in Multi-Modal Embeddings 3009
Tingwei Zhang and Rishi Jha, *Cornell University;* Eugene Bagdasaryan, *University of Massachusetts Amherst;* Vitaly Shmatikov, *Cornell Tech*

It Doesn't Look Like Anything to Me: Using Diffusion Model to Subvert Visual Phishing Detectors 3027
Qingying Hao and Nirav Diwan, *University of Illinois at Urbana-Champaign;* Ying Yuan, *University of Padua;* Giovanni Apruzzese, *University of Liechtenstein;* Mauro Conti, *University of Padua;* Gang Wang, *University of Illinois at Urbana-Champaign*

Invisibility Cloak: Proactive Defense Against Visual Game Cheating 3045
Chenxin Sun, Kai Ye, Liangcai Su, Jiayi Zhang, and Chenxiong Qian, *The University of Hong Kong*

Security Analysis III: Protocol

Logic Gone Astray: A Security Analysis Framework for the Control Plane Protocols of 5G Basebands 3063
Kai Tu, Abdullah Al Ishtiaq, Syed Md Mukit Rashid, Yilu Dong, Weixuan Wang, Tianwei Wu, and Syed Rafiul Hussain, *Pennsylvania State University*

SPF Beyond the Standard: Management and Operational Challenges in Practice and Practical Recommendations . . 3081
Md. Ishtiaq Ashiq and Weitong Li, *Virginia Tech;* Tobias Fiebig, *Max-Planck-Institut für Informatik;* Taejoong Chung, *Virginia Tech*

A Formal Analysis of SCTP: Attack Synthesis and Patch Verification 3099
Jacob Ginesin, Max von Hippel, Evan Defloor, and Cristina Nita-Rotaru, *Northeastern University;* Michael Tüxen, *FH Münster*

Athena: Analyzing and Quantifying Side Channels of Transport Layer Protocols 3117
Feiyang Yu, *Duke University;* Quan Zhou and Syed Rafiul Hussain, *Pennsylvania State University;* Danfeng Zhang, *Duke University*

Shaken, not Stirred - Automated Discovery of Subtle Attacks on Protocols using Mix-Nets 3135
Jannik Dreier, *Université de Lorraine, CNRS, Inria, LORIA;* Pascal Lafourcade and Dhekra Mahmoud, *Université de Clermont Auvergne, LIMOS*

Cryptographic Protocols II

Rabbit-Mix: Robust Algebraic Anonymous Broadcast from Additive Bases 3151
Chongwon Cho and Samuel Dittmer, *Stealth Software Technologies Inc.;* Yuval Ishai, *Technion;* Steve Lu, *Stealth Software Technologies Inc.;* Rafail Ostrovsky, *UCLA*

PerfOMR: Oblivious Message Retrieval with Reduced Communication and Computation 3169
Zeyu Liu, *Yale University;* Eran Tromer, *Boston University;* Yunhao Wang, *Yale University*

Fast RS-IOP Multivariate Polynomial Commitments and Verifiable Secret Sharing. 3187
Zongyang Zhang, Weihan Li, Yanpei Guo, and Kexin Shi, *Beihang University;* Sherman S. M. Chow, *The Chinese University of Hong Kong;* Ximeng Liu, *Fuzhou University;* Jin Dong, *Beijing Academy of Blockchain and Edge Computing*

Abuse Reporting for Metadata-Hiding Communication Based on Secret Sharing 3205
Saba Eskandarian, *University of North Carolina at Chapel Hill*

SOAP: A Social Authentication Protocol 3223
Felix Linker and David Basin, *Department of Computer Science, ETH Zurich*

User Studies IV: Policies and Best Practices I

How WEIRD is Usable Privacy and Security Research? 3241
Ayako A. Hasegawa and Daisuke Inoue, *NICT;* Mitsuaki Akiyama, *NTT*

Security and Privacy Software Creators' Perspectives on Unintended Consequences 3259
Harshini Sri Ramulu, *Paderborn University & The George Washington University;* Helen Schmitt, *Paderborn University;* Dominik Wermke, *North Carolina State University;* Yasemin Acar, *Paderborn University & The George Washington University*

Engaging Company Developers in Security Research Studies: A Comprehensive Literature Review and Quantitative Survey. 3277
Raphael Serafini, Stefan Albert Horstmann, and Alena Naiakshina, *Ruhr University Bochum*

"What Keeps People Secure is That They Met The Security Team": Deconstructing Drivers And Goals of Organizational Security Awareness 3295
Jonas Hielscher, *Ruhr University Bochum;* Simon Parkin, *Delft University of Technology*

Unveiling the Hunter-Gatherers: Exploring Threat Hunting Practices and Challenges in Cyber Defense 3313
Priyanka Badva, Kopo M. Ramokapane, Eleonora Pantano, and Awais Rashid, *University of Bristol*

Side Channel IV

Pixel Thief: Exploiting SVG Filter Leakage in Firefox and Chrome 3331
Sioli O'Connell, *The University of Adelaide;* Lishay Aben Sour and Ron Magen, *Ben Gurion University of the Negev;* Daniel Genkin, *Georgia Institute of Technology;* Yossi Oren, *Ben-Gurion University of the Negev and Intel Corporation;* Hovav Shacham, *UT Austin;* Yuval Yarom, *Ruhr University Bochum*

Sync+Sync: A Covert Channel Built on fsync with Storage 3349
Qisheng Jiang and Chundong Wang, *ShanghaiTech University*

What Was Your Prompt? A Remote Keylogging Attack on AI Assistants 3367
Roy Weiss, Daniel Ayzenshteyn, Guy Amit, and Yisroel Mirsky, *Ben Gurion University of the Negev*

NetShaper: A Differentially Private Network Side-Channel Mitigation System 3385
Amir Sabzi, Rut Vora, Swati Goswami, Margo Seltzer, Mathias Lécuyer, and Aastha Mehta, *University of British Columbia*

SoK: Neural Network Extraction Through Physical Side Channels 3403
Péter Horváth, Dirk Lauret, Zhuoran Liu, and Lejla Batina, *Radboud University*

Cloud Security

ACAI: Protecting Accelerator Execution with Arm Confidential Computing Architecture 3423
Supraja Sridhara, Andrin Bertschi, Benedict Schlüter, Mark Kuhne, Fabio Aliberti, and Shweta Shinde, *ETH Zurich*

***ChainPatrol*: Balancing Attack Detection and Classification with Performance Overhead for Service Function Chains Using Virtual Trailers 3441**
Momen Oqaily and Hinddeep Purohit, *CIISE, Concordia University;* Yosr Jarraya, *Ericsson Security Research;* Lingyu Wang, *CIISE, Concordia University;* Boubakr Nour and Makan Pourzandi, *Ericsson Security Research;* Mourad Debbabi, *CIISE, Concordia University*

HECKLER: Breaking Confidential VMs with Malicious Interrupts 3459
Benedict Schlüter, Supraja Sridhara, Mark Kuhne, Andrin Bertschi, and Shweta Shinde, *ETH Zurich*

Stateful Least Privilege Authorization for the Cloud 3477
Leo Cao, Luoxi Meng, Deian Stefan, and Earlence Fernandes, *UC San Diego*

GraphGuard: Private Time-Constrained Pattern Detection Over Streaming Graphs in the Cloud 3495
Songlei Wang and Yifeng Zheng, *Harbin Institute of Technology;* Xiaohua Jia, *Harbin Institute of Technology and City University of Hong Kong*

Blockchain I

Mempool Privacy via Batched Threshold Encryption: Attacks and Defenses 3513
Arka Rai Choudhuri, *NTT Research;* Sanjam Garg, Julien Piet, and Guru-Vamsi Policharla, *University of California, Berkeley*

Speculative Denial-of-Service Attacks In Ethereum 3531
Aviv Yaish, *The Hebrew University;* Kaihua Qin and Liyi Zhou, *Imperial College London, UC Berkeley RDI;* Aviv Zohar, *The Hebrew University;* Arthur Gervais, *University College London, UC Berkeley RDI*

GuideEnricher: Protecting the Anonymity of Ethereum Mixing Service Users with Deep Reinforcement Learning . . 3549
Ravindu De Silva, Wenbo Guo, Nicola Ruaro, Ilya Grishchenko, Christopher Kruegel, and Giovanni Vigna, *University of California, Santa Barbara*

All Your Tokens are Belong to Us: Demystifying Address Verification Vulnerabilities in Solidity Smart Contracts . . 3567
Tianle Sun, *Huazhong University of Science and Technology;* Ningyu He, *Peking University;* Jiang Xiao, *Huazhong University of Science and Technology;* Yinliang Yue, *Zhongguancun Laboratory;* Xiapu Luo, *The Hong Kong Polytechnic University;* Haoyu Wang, *Huazhong University of Science and Technology*

Using My Functions Should Follow My Checks: Understanding and Detecting Insecure OpenZeppelin Code in Smart Contracts 3585
Han Liu, *East China Normal University, Shanghai Key Laboratory of Trustworthy Computing;* Daoyuan Wu, *The Hong Kong University of Science and Technology;* Yuqiang Sun, *Nanyang Technological University;* Haijun Wang, *Xi'an Jiaotong University;* Kaixuan Li, *East China Normal University, Shanghai Key Laboratory of Trustworthy Computing;* Yang Liu, *Nanyang Technological University;* Yixiang Chen, *East China Normal University, Shanghai Key Laboratory of Trustworthy Computing*

ML VII: Adversarial Attack Defense

Correction-based Defense Against Adversarial Video Attacks via Discretization-Enhanced Video Compressive Sensing 3603
Wei Song, Cong Cong, Haonan Zhong, and Jingling Xue, *UNSW Sydney*

Rethinking the Invisible Protection against Unauthorized Image Usage in Stable Diffusion 3621
Shengwei An, Lu Yan, Siyuan Cheng, Guangyu Shen, Kaiyuan Zhang, Qiuling Xu, Guanhong Tao, and Xiangyu Zhang, *Purdue University*

Splitting the Difference on Adversarial Training 3639
Matan Levi and Aryeh Kontorovich, *Ben-Gurion University of the Negev*

Machine Learning needs Better Randomness Standards: *Randomised Smoothing* and PRNG-based attacks 3657
Pranav Dahiya, *University of Cambridge;* Ilia Shumailov, *University of Oxford;* Ross Anderson, *University of Cambridge & University of Edinburgh*

PATCHCURE: Improving Certifiable Robustness, Model Utility, and Computation Efficiency of Adversarial Patch Defenses 3675
Chong Xiang, Tong Wu, and Sihui Dai, *Princeton University;* Jonathan Petit, *Qualcomm Technologies, Inc.;* Suman Jana, *Columbia University;* Prateek Mittal, *Princeton University*

Language-Based Security

GHunter: Universal Prototype Pollution Gadgets in JavaScript Runtimes 3693
Eric Cornelissen, Mikhail Shcherbakov, and Musard Balliu, *KTH Royal Institute of Technology*

MetaSafe: Compiling for Protecting Smart Pointer Metadata to Ensure Safe Rust Integrity 3711
Martin Kayondo and Inyoung Bang, *Seoul National University;* Yeongjun Kwak and Hyungon Moon, *UNIST;* Yunheung Paek, *Seoul National University*

RustSan: Retrofitting AddressSanitizer for Efficient Sanitization of Rust 3729
Kyuwon Cho, Jongyoon Kim, Kha Dinh Duy, Hajeong Lim, and Hojoon Lee, *Sungkyunkwan University*

FV8: A Forced Execution JavaScript Engine for Detecting Evasive Techniques 3747
Nikolaos Pantelaios and Alexandros Kapravelos, *North Carolina State University*

Donapi: Malicious NPM Packages Detector using Behavior Sequence Knowledge Mapping 3765
Cheng Huang, Nannan Wang, Ziyan Wang, Siqi Sun, Lingzi Li, Junren Chen, Qianchong Zhao, Jiaxuan Han, and Zhen Yang, *Sichuan University;* Lei Shi, *Huawei Technologies*

Zero-Knowledge Proof II

Election Eligibility with OpenID: Turning Authentication into Transferable Proof of Eligibility 3783
Véronique Cortier, Alexandre Debant, Anselme Goetschmann, and Lucca Hirschi, *Université de Lorraine, CNRS, Inria, LORIA, France*

Reef: Fast Succinct Non-Interactive Zero-Knowledge Regex Proofs 3801
Sebastian Angel, Eleftherios Ioannidis, and Elizabeth Margolin, *University of Pennsylvania;* Srinath Setty, *Microsoft Research;* Jess Woods, *University of Pennsylvania*

Scalable Zero-knowledge Proofs for Non-linear Functions in Machine Learning 3819
Meng Hao, Hanxiao Chen, and Hongwei Li, *School of Computer Science and Engineering, University of Electronic Science and Technology of China;* Chenkai Weng, *Northwestern University;* Yuan Zhang and Haomiao Yang, *School of Computer Science and Engineering, University of Electronic Science and Technology of China;* Tianwei Zhang, *Nanyang Technological University*

ZKSMT: A VM for Proving SMT Theorems in Zero Knowledge 3837
Daniel Luick, John C. Kolesar, and Timos Antonopoulos, *Yale University;* William R. Harris and James Parker, *Galois, Inc.;* Ruzica Piskac, *Yale University;* Eran Tromer, *Boston University;* Xiao Wang and Ning Luo, *Northwestern University*

SoK: What Don't We Know? Understanding Security Vulnerabilities in SNARKs 3855
Stefanos Chaliasos, *Imperial College London;* Jens Ernstberger; David Theodore, *Ethereum Foundation;* David Wong, *zkSecurity;* Mohammad Jahanara, *Scroll Foundation;* Benjamin Livshits, *Imperial College London & Matter Labs*

Measurement III: Auditing and Best Practices I

SecurityNet: Assessing Machine Learning Vulnerabilities on Public Models 3873
Boyang Zhang, Zheng Li, Ziqing Yang, Xinlei He, Michael Backes, Mario Fritz, and Yang Zhang, *CISPA Helmholtz Center for Information Security*

How does Endpoint Detection use the MITRE ATT&CK Framework? 3891
Apurva Virkud, Muhammad Adil Inam, Andy Riddle, Jason Liu, Gang Wang, and Adam Bates, *University of Illinois Urbana-Champaign*

Digital Discrimination of Users in Sanctioned States: The Case of the Cuba Embargo 3909
Anna Ablove, Shreyas Chandrashekaran, Hieu Le, Ram Sundara Raman, and Reethika Ramesh, *University of Michigan;* Harry Oppenheimer, *Georgia Institute of Technology;* Roya Ensafi, *University of Michigan*

A Broad Comparative Evaluation of Software Debloating Tools 3927
Michael D. Brown and Adam Meily, *Trail of Bits;* Brian Fairservice, Akshay Sood, and Jonathan Dorn, *GrammaTech;* Eric Kilmer and Ronald Eytchison, *Trail of Bits*

Hardware Security III: Signals

LaserAdv: Laser Adversarial Attacks on Speech Recognition Systems 3945
Guoming Zhang, Xiaohui Ma, Huiting Zhang, and Zhijie Xiang, *Shandong University;* Xiaoyu Ji, *Zhejiang University;* Yanni Yang, Xiuzhen Cheng, and Pengfei Hu, *Shandong University*

MicGuard: A Comprehensive Detection System against Out-of-band Injection Attacks for Different Level Microphone-based Devices. 3963
Tiantian Liu, Feng Lin, Zhongjie Ba, Li Lu, Zhan Qin, and Kui Ren, *Zhejiang University and Hangzhou High-Tech Zone (Binjiang) Institute of Blockchain and Data Security*

***VoltSchemer*: Use Voltage Noise to Manipulate Your Wireless Charger 3979**
Zihao Zhan and Yirui Yang, *University of Florida;* Haoqi Shan, *University of Florida, CertiK;* Hanqiu Wang, Yier Jin, and Shuo Wang, *University of Florida*

VibSpeech: Exploring Practical Wideband Eavesdropping via Bandlimited Signal of Vibration-based Side Channel 3997
Chao Wang, Feng Lin, Hao Yan, and Tong Wu, *Zhejiang University;* Wenyao Xu, *University at Buffalo, the State University of New York;* Kui Ren, *Zhejiang University*

System Security III: Memory I

CAMP: Compiler and Allocator-based Heap Memory Protection 4015
Zhenpeng Lin, Zheng Yu, Ziyi Guo, Simone Campanoni, Peter Dinda, and Xinyu Xing, *Northwestern University*

GPU Memory Exploitation for Fun and Profit 4033
Yanan Guo, *University of Rochester;* Zhenkai Zhang, *Clemson University;* Jun Yang, *University of Pittsburgh*

SLUBStick: Arbitrary Memory Writes through Practical Software Cross-Cache Attacks within the Linux Kernel 4051
Lukas Maar, Stefan Gast, Martin Unterguggenberger, Mathias Oberhuber, and Stefan Mangard, *Graz University of Technology*

Detecting Kernel Memory Bugs through Inconsistent Memory Management Intention Inferences 4069
Dinghao Liu, Zhipeng Lu, and Shouling Ji, *Zhejiang University;* Kangjie Lu, *University of Minnesota;* Jianhai Chen and Zhenguang Liu, *Zhejiang University;* Dexin Liu, *Peking University;* Renyi Cai, *Alibaba Cloud Computing Co., Ltd;* Qinming He, *Zhejiang University*

Web Security II: Privacy

Near-Optimal Constrained Padding for Object Retrievals with Dependencies 4087
Pranay Jain, *Duke University;* Andrew C. Reed, *United States Military Academy;* Michael K. Reiter, *Duke University*

PURL: Safe and Effective Sanitization of Link Decoration 4103
Shaoor Munir and Patrick Lee, *University of California, Davis;* Umar Iqbal, *Washington University in St. Louis;* Zubair Shafiq, *University of California, Davis;* Sandra Siby, *Imperial College London*

Fledging Will Continue Until Privacy Improves: Empirical Analysis of Google's Privacy-Preserving Targeted Advertising 4121
Giuseppe Calderonio, Mir Masood Ali, and Jason Polakis, *University of Illinois Chicago*

Stop, Don't Click Here Anymore: Boosting Website Fingerprinting By Considering Sets of Subpages 4139
Asya Mitseva and Andriy Panchenko, *Brandenburg University of Technology* (*BTU Cottbus, Germany*)

ML VIII: Backdoors and Federated Learning

Lurking in the shadows: Unveiling Stealthy Backdoor Attacks against Personalized Federated Learning 4157
Xiaoting Lyu, *Beijing Jiaotong University;* Yufei Han, *INRIA;* Wei Wang, Jingkai Liu, and Yongsheng Zhu, *Beijing Jiaotong University;* Guangquan Xu, *Tianjin University;* Jiqiang Liu, *Beijing Jiaotong University;* Xiangliang Zhang, *University of Notre Dame*

ACE: A Model Poisoning Attack on Contribution Evaluation Methods in Federated Learning 4175
Zhangchen Xu, Fengqing Jiang, and Luyao Niu, *University of Washington;* Jinyuan Jia, *Pennsylvania State University;* Bo Li, *University of Chicago;* Radha Poovendran, *University of Washington*

BackdoorIndicator: Leveraging OOD Data for Proactive Backdoor Detection in Federated Learning 4193
Songze Li, *Southeast University;* Yanbo Dai, *HKUST*(*GZ*)

UBA-Inf: Unlearning Activated Backdoor Attack with Influence-Driven Camouflage 4211
Zirui Huang, Yunlong Mao, and Sheng Zhong, *Nanjing University*

Software Security + ML 1

Racing on the Negative Force: Efficient Vulnerability Root-Cause Analysis through Reinforcement Learning on Counterexamples 4229
Dandan Xu, *SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, China, and School of Cyber Security, University of Chinese Academy of Sciences, China;* Di Tang, Yi Chen, and XiaoFeng Wang, *Indiana University Bloomington;* Kai Chen, *SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, China, and School of Cyber Security, University of Chinese Academy of Sciences, China;* Haixu Tang, *Indiana University Bloomington;* Longxing Li, *SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, China, and School of Cyber Security, University of Chinese Academy of Sciences, China*

Uncovering the Limits of Machine Learning for Automatic Vulnerability Detection 4247
Niklas Risse and Marcel Böhme, *MPI-SP, Germany*

Improving ML-based Binary Function Similarity Detection by Assessing and Deprioritizing Control Flow Graph Features 4265
Jialai Wang, *Tsinghua University;* Chao Zhang, *Tsinghua University and Zhongguancun Laboratory;* Longfei Chen and Yi Rong, *Tsinghua University;* Yuxiao Wu, *Huazhong University of Science and Technology;* Hao Wang, Wende Tan, and Qi Li, *Tsinghua University;* Zongpeng Li, *Tsinghua University and Quancheng Labs*

TyGr: Type Inference on Stripped Binaries using Graph Neural Networks 4283
Chang Zhu, *Arizona State University;* Ziyang Li and Anton Xue, *University of Pennsylvania;* Ati Priya Bajaj, Wil Gibbs, and Yibo Liu, *Arizona State University;* Rajeev Alur, *University of Pennsylvania;* Tiffany Bao, *Arizona State University;* Hanjun Dai, *Google;* Adam Doupé, *Arizona State University;* Mayur Naik, *University of Pennsylvania;* Yan Shoshitaishvili and Ruoyu Wang, *Arizona State University;* Aravind Machiry, *Purdue University*

Crypto III: Password and Secret Key

MFKDF: Multiple Factors Knocked Down Flat 4301
Matteo Scarlata and Matilda Backendal, *ETH Zurich;* Miro Haller, *UC San Diego*

LaKey: Efficient Lattice-Based Distributed PRFs Enable Scalable Distributed Key Management 4319
Matthias Geihs, *Torus Labs;* Hart Montgomery, *Linux Foundation*

Exploiting Leakage in Password Managers via Injection Attacks. 4337
Andrés Fábrega, Armin Namavari, and Rachit Agarwal, *Cornell University;* Ben Nassi, *Cornell Tech, Technion - Israel Institute of Technology;* Thomas Ristenpart, *Cornell University, Cornell Tech*

OPTIKS: An Optimized Key Transparency System 4355
Julia Len, *Cornell Tech;* Melissa Chase, Esha Ghosh, Kim Laine, and Radames Cruz Moreno, *Microsoft Research*

Social Issues III: Social Media Platform

Understanding the Security and Privacy Implications of Online Toxic Content on Refugees 4373
Arjun Arunasalam, *Purdue University;* Habiba Farrukh, *University of California, Irvine;* Eliz Tekcan and Z. Berkay Celik, *Purdue University*

Understanding Help-Seeking and Help-Giving on Social Media for Image-Based Sexual Abuse 4391
Miranda Wei, *University of Washington / Google;* Sunny Consolvo and Patrick Gage Kelley, *Google;* Tadayoshi Kohno, *University of Washington;* Tara Matthews and Sarah Meiklejohn, *Google;* Franziska Roesner, *University of Washington;* Renee Shelby, Kurt Thomas, and Rebecca Umbach, *Google*

Enabling Contextual Soft Moderation on Social Media through Contrastive Textual Deviation 4409
Pujan Paudel, Mohammad Hammas Saeed, Rebecca Auger, Chris Wells, and Gianluca Stringhini, *Boston University*

The Imitation Game: Exploring Brand Impersonation Attacks on Social Media Platforms 4427
Bhupendra Acharya, *CISPA Helmholtz Center for Information Security;* Dario Lazzaro, *University of Genoa;* Efrén López-Morales, *Texas A&M University-Corpus Christi;* Adam Oest and Muhammad Saad, *PayPal Inc.;* Antonio Emanuele Cinà, *University of Genoa;* Lea Schönherr and Thorsten Holz, *CISPA Helmholtz Center for Information Security*

Wireless Security I: Cellular and Bluetooth

Hermes: Unlocking Security Analysis of Cellular Network Protocols by Synthesizing Finite State Machines from Natural Language Specifications **4445**
Abdullah Al Ishtiaq, Sarkar Snigdha Sarathi Das, Syed Md Mukit Rashid, Ali Ranjbar, Kai Tu, Tianwei Wu, Zhezheng Song, Weixuan Wang, Mujtahid Akon, Rui Zhang, and Syed Rafiul Hussain, *Pennsylvania State University*

On the Criticality of Integrity Protection in 5G Fronthaul Networks. **4463**
Jiarong Xing, *Rice University;* Sophia Yoo, *Princeton University;* Xenofon Foukas, *Microsoft;* Daehyeok Kim, *The University of Texas at Austin;* Michael K. Reiter, *Duke University*

SIMurai: Slicing Through the Complexity of SIM Card Security Research **4481**
Tomasz Piotr Lisowski, *University of Birmingham;* Merlin Chlosta, *CISPA Helmholtz Center for Information Security;* Jinjin Wang and Marius Muench, *University of Birmingham*

Finding Traceability Attacks in the Bluetooth Low Energy Specification and Its Implementations. **4499**
Jianliang Wu, *Purdue University & Simon Fraser University;* Patrick Traynor, *University of Florida;* Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi, *Purdue University*

Mobile Security II

Defects-in-Depth: Analyzing the Integration of Effective Defenses against One-Day Exploits in Android Kernels . . . **4517**
Lukas Maar, *Graz University of Technology;* Florian Draschbacher, *Graz University of Technology and A-SIT Austria, Graz;* Lukas Lamster and Stefan Mangard, *Graz University of Technology*

Exploring Covert Third-party Identifiers through External Storage in the Android New Era **4535**
Zikan Dong, *Beijing University of Posts and Telecommunications;* Tianming Liu, *Monash University/Huazhong University of Science and Technology;* Jiapeng Deng and Haoyu Wang, *Huazhong University of Science and Technology;* Li Li, *Beihang University;* Minghui Yang and Meng Wang, *OPPO;* Guosheng Xu, *Beijing University of Posts and Telecommunications;* Guoai Xu, *Harbin Institute of Technology, Shenzhen*

PURE: Payments with UWB RElay-protection **4553**
Daniele Coppola, Giovanni Camurati, Claudio Anliker, Xenia Hofmeier, Patrick Schaller, David Basin, and Srdjan Capkun, *ETH Zurich*

***Do You See How I Pose?* Using Poses as an Implicit Authentication Factor for QR Code Payment.** **4571**
Chuxiong Wu and Qiang Zeng, *George Mason University*

Measurement IV: Web

Simulated Stress: A Case Study of the Effects of a Simulated Phishing Campaign on Employees' Perception, Stress and Self-Efficacy **4589**
Markus Schöps, Marco Gutfleisch, Eric Wolter, and M. Angela Sasse, *Ruhr University Bochum*

Arcanum: Detecting and Evaluating the Privacy Risks of Browser Extensions on Web Pages and Web Content . . . **4607**
Qinge Xie, Manoj Vignesh Kasi Murali, Paul Pearce, and Frank Li, *Georgia Institute of Technology*

Smudged Fingerprints: Characterizing and Improving the Performance of Web Application Fingerprinting **4625**
Brian Kondracki and Nick Nikiforakis, *Stony Brook University*

Does Online Anonymous Market Vendor Reputation Matter? **4641**
Alejandro Cuevas and Nicolas Christin, *Carnegie Mellon University*

LLM II: Jailbreaking

LLM-Fuzzer: Scaling Assessment of Large Language Model Jailbreaks **4657**
Jiahao Yu, *Northwestern University;* Xingwei Lin, *Ant Group;* Zheng Yu and Xinyu Xing, *Northwestern University*

Don't Listen To Me: Understanding and Exploring Jailbreak Prompts of Large Language Models **4675**
Zhiyuan Yu, *Washington University in St. Louis;* Xiaogeng Liu, *University of Wisconsin, Madison;* Shunning Liang, *Washington University in St. Louis;* Zach Cameron, *John Burroughs School;* Chaowei Xiao, *University of Wisconsin, Madison;* Ning Zhang, *Washington University in St. Louis*

***Malla*: Demystifying Real-world Large Language Model Integrated Malicious Services** **4693**
Zilong Lin, Jian Cui, Xiaojing Liao, and XiaoFeng Wang, *Indiana University Bloomington*

Making Them Ask and Answer: Jailbreaking Large Language Models in Few Queries via Disguise and Reconstruction 4711
Tong Liu and Yingjie Zhang, *Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences;* Zhe Zhao, *RealAI;* Yinpeng Dong, *RealAI and Tsinghua University;* Guozhu Meng and Kai Chen, *Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences*

Fuzzing III: Network

ResolverFuzz: Automated Discovery of DNS Resolver Vulnerabilities with Query-Response Fuzzing 4729
Qifan Zhang and Xuesong Bai, *University of California, Irvine;* Xiang Li, *Tsinghua University;* Haixin Duan, *Tsinghua University; Zhongguancun Laboratory; Quan Cheng Laboratory;* Qi Li, *Tsinghua University;* Zhou Li, *University of California, Irvine*

Understanding Ethereum Mempool Security under Asymmetric DoS by Symbolized Stateful Fuzzing 4747
Yibo Wang and Yuzhe Tang, *Syracuse University;* Kai Li, *San Diego State University;* Wanning Ding and Zhihua Yang, *Syracuse University*

Atropos: Effective Fuzzing of Web Applications for Server-Side Vulnerabilities 4765
Emre Güler and Sergej Schumilo, *Ruhr University Bochum;* Moritz Schloegel, Nils Bars, Philipp Görz, and Xinyi Xu, *CISPA Helmholtz Center for Information Security;* Cemal Kaygusuz, *Ruhr University Bochum;* Thorsten Holz, *CISPA Helmholtz Center for Information Security*

***From One Thousand Pages of Specification to Unveiling Hidden Bugs:* Large Language Model Assisted Fuzzing of Matter IoT Devices 4783**
Xiaoyue Ma, Lannan Luo, and Qiang Zeng, *George Mason University*

Differential Privacy II

DAAP: Privacy-Preserving Model Accuracy Estimation on Unlabeled Datasets Through Distribution-Aware Adversarial Perturbation 4801
Guodong Cao, *Wuhan University;* Zhibo Wang, *Zhejiang University;* Yunhe Feng, *University of North Texas;* Xiaowei Dong, *Wuhan University*

Closed-Form Bounds for DP-SGD against Record-level Inference Attacks 4819
Giovanni Cherubin, *Microsoft Security Response Center;* Boris Köpf, *Microsoft Azure Research;* Andrew Paverd, *Microsoft Security Response Center;* Shruti Tople, *Microsoft Azure Research;* Lukas Wutschitz, *Microsoft M365 Research;* Santiago Zanella-Béguelin, *Microsoft Azure Research*

PrivImage: Differentially Private Synthetic Image Generation using Diffusion Models with Semantic-Aware Pretraining 4837
Kecen Li, *Institute of Automation, Chinese Academy of Sciences and University of Chinese Academy of Sciences;* Chen Gong, *University of Virginia;* Zhixiang Li, *University of Bristol;* Yuzhong Zhao, *University of Chinese Academy of Sciences;* Xinwen Hou, *Institute of Automation, Chinese Academy of Sciences;* Tianhao Wang, *University of Virginia*

"What do you want from theory alone?" Experimenting with Tight Auditing of Differentially Private Synthetic Data Generation 4855
Meenatchi Sundaram Muthu Selva Annamalai, *University College London;* Georgi Ganev, *University College London and Hazy;* Emiliano De Cristofaro, *University of California, Riverside*

Friday, August 16

User Studies V: Policies and Best Practices II

"I Don't Know If We're Doing Good. I Don't Know If We're Doing Bad": Investigating How Practitioners Scope, Motivate, and Conduct Privacy Work When Developing AI Products 4873
Hao-Ping (Hank) Lee, *Carnegie Mellon University;* Lan Gao and Stephanie Yang, *Georgia Institute of Technology;* Jodi Forlizzi and Sauvik Das, *Carnegie Mellon University*

Towards More Practical Threat Models in Artificial Intelligence Security 4891
Kathrin Grosse, *EPFL;* Lukas Bieringer, *QuantPi;* Tarek R. Besold, *TU Eindhoven;* Alexandre M. Alahi, *EPFL*

"There are rabbit holes I want to go down that I'm not allowed to go down": An Investigation of Security Expert Threat Modeling Practices for Medical Devices 4909
Ronald E. Thompson, Madline McLaughlin, Carson Powers, and Daniel Votipka, *Tufts University*

"*Belt and suspenders*" or "*just red tape*"?: Investigating Early Artifacts and User Perceptions of IoT App Security Certification 4927
Prianka Mandal, Amit Seal Ami, Victor Olaiya, Sayyed Hadi Razmjo, and Adwait Nadkarni, *William & Mary*

TAPFixer: Automatic Detection and Repair of Home Automation Vulnerabilities based on Negated-property Reasoning. 4945
Yinbo Yu, *National Engineering Laboratory for Integrated Aero-Space-Ground-Ocean Big Data Application Technology, School of Cybersecurity, Northwestern Polytechnical University, China; Research & Development Institute of Northwestern Polytechnical University in Shenzhen, China;* Yuanqi Xu, Kepu Huang, and Jiajia Liu, *National Engineering Laboratory for Integrated Aero-Space-Ground-Ocean Big Data Application Technology, School of Cybersecurity, Northwestern Polytechnical University, China*

User Studies VI: Privacy II

Co-Designing a Mobile App for Bystander Privacy Protection in Jordanian Smart Homes: A Step Towards Addressing a Complex Privacy Landscape 4963
Wael Albayaydh and Ivan Flechais, *University of Oxford*

"I really just leaned on my community for support": Barriers, Challenges, and Coping Mechanisms Used by Survivors of Technology-Facilitated Abuse to Seek Social Support 4981
Naman Gupta, *University of Wisconsin–Madison, Madison Tech Clinic;* Kate Walsh, *University of Wisconsin–Madison;* Sanchari Das, *University of Denver;* Rahul Chatterjee, *University of Wisconsin–Madison, Madison Tech Clinic*

From the Childhood Past: Views of Young Adults on Parental Sharing of Children's Photos. 4999
Tania Ghafourian, *Indiana University Bloomington;* Nicholas Micallef, *Swansea University;* Sameer Patil, *University of Utah*

ATTention Please! An Investigation of the App Tracking Transparency Permission. 5017
Reham Mohamed and Arjun Arunasalam, *Purdue University;* Habiba Farrukh, *University of California, Irvine;* Jason Tong, Antonio Bianchi, and Z. Berkay Celik, *Purdue University*

Voice App Developer Experiences with Alexa and Google Assistant: Juggling Risks, Liability, and Security. 5035
William Seymour, *King's College London;* Noura Abdi, *Liverpool Hope University;* Kopo M. Ramokapane, *University of Bristol;* Jide Edu, *University of Strathclyde;* Guillermo Suarez-Tangil, *IMDEA Networks Institute;* Jose Such, *King's College London & Universitat Politecnica de Valencia*

Measurement V: App

Swipe Left for Identity Theft: An Analysis of User Data Privacy Risks on Location-based Dating Apps 5053
Karel Dhondt, Victor Le Pochat, Yana Dimova, Wouter Joosen, and Stijn Volckaert, *DistriNet, KU Leuven*

Spill the TeA: An Empirical Study of Trusted Application Rollback Prevention on Android Smartphones 5071
Marcel Busch, Philipp Mao, and Mathias Payer, *EPFL*

A Decade of Privacy-Relevant Android App Reviews: Large Scale Trends 5089
Omer Akgul, *University of Maryland;* Sai Teja Peddinti and Nina Taft, *Google;* Michelle L. Mazurek, *University of Maryland;* Hamza Harkous, Animesh Srivastava, and Benoit Seguin, *Google*

Tickets or Privacy? Understand the Ecosystem of Chinese Ticket Grabbing Apps 5107
Yijing Liu and Yiming Zhang, *Tsinghua University;* Baojun Liu, *Tsinghua University; Zhongguancun Laboratory;* Haixin Duan, *Tsinghua University; Quancheng Laboratory;* Qiang Li, *Qihoo 360;* Mingxuan Liu, *Zhongguancun Laboratory;* Ruixuan Li and Jia Yao, *Tsinghua University*

PixelMod: Improving Soft Moderation of Visual Misleading Information on Twitter 5125
Pujan Paudel and Chen Ling, *Boston University;* Jeremy Blackburn, *Binghamton University;* Gianluca Stringhini, *Boston University*

Network Security III: Detection

Learning with Semantics: Towards a Semantics-Aware Routing Anomaly Detection System 5143
Yihao Chen, *Department of Computer Science and Technology & BNRist, Tsinghua University;* Qilei Yin, *Zhongguancun Laboratory;* Qi Li and Zhuotao Liu, *Institute for Network Sciences and Cyberspace, Tsinghua University; Zhongguancun Laboratory;* Ke Xu, *Department of Computer Science and Technology, Tsinghua University; Zhongguancun Laboratory;* Yi Xu and Mingwei Xu, *Institute for Network Sciences and Cyberspace, Tsinghua University; Zhongguancun Laboratory;* Ziqian Liu, *China Telecom;* Jianping Wu, *Department of Computer Science and Technology, Tsinghua University; Zhongguancun Laboratory*

Enhancing Network Attack Detection with Distributed and In-Network Data Collection System 5161
Seyed Mohammad Mehdi Mirnajafizadeh and Ashwin Raam Sethuram, *Wayne State University;* David Mohaisen, *University of Central Florida;* DaeHun Nyang, *Ewha Womans University;* Rhongho Jang, *Wayne State University*

You Cannot Escape Me: Detecting Evasions of SIEM Rules in Enterprise Networks 5179
Rafael Uetz, Marco Herzog, and Louis Hackländer, *Fraunhofer FKIE;* Simon Schwarz, *University of Göttingen;* Martin Henze, *RWTH Aachen University & Fraunhofer FKIE*

MAGIC: Detecting Advanced Persistent Threats via Masked Graph Representation Learning 5197
Zian Jia and Yun Xiong, *Shanghai Key Laboratory of Data Science, School of Computer Science, Fudan University, China;* Yuhong Nan, *School of Software Engineering, Sun Yat-sen University, China;* Yao Zhang, *Shanghai Key Laboratory of Data Science, School of Computer Science, Fudan University, China;* Jinjing Zhao, *National Key Laboratory of Science and Technology on Information System Security, China;* Mi Wen, *Shanghai University of Electric Power, China*

CellularLint: A Systematic Approach to Identify Inconsistent Behavior in Cellular Network Specifications 5215
Mirza Masfiqur Rahman, Imtiaz Karim, and Elisa Bertino, *Purdue University*

ML IX: Model Extraction and Watermark

SoK: All You Need to Know About On-Device ML Model Extraction - The Gap Between Research and Practice . . 5233
Tushar Nayan, Qiming Guo, and Mohammed Al Duniawi, *Florida International University;* Marcus Botacin, *Texas A&M University;* Selcuk Uluagac and Ruimin Sun, *Florida International University*

Unveiling the Secrets without Data: Can Graph Neural Networks Be Exploited through Data-Free Model Extraction Attacks? 5251
Yuanxin Zhuang, Chuan Shi, and Mengmei Zhang, *Beijing University of Posts and Telecommunications;* Jinghui Chen, *The Pennsylvania State University;* Lingjuan Lyu, *SONY AI;* Pan Zhou, *Huazhong University of Science and Technology;* Lichao Sun, *Lehigh University*

ClearStamp: A Human-Visible and Robust Model-Ownership Proof based on Transposed Model Training 5269
Torsten Krauß, Jasper Stang, and Alexandra Dmitrienko, *University of Würzburg*

***DeepEclipse*: How to Break White-Box DNN-Watermarking Schemes 5287**
Alessandro Pegoraro, Carlotta Segna, Kavita Kumari, and Ahmad-Reza Sadeghi, *Technical University of Darmstadt*

ModelGuard: Information-Theoretic Defense Against Model Extraction Attacks 5305
Minxue Tang and Anna Dai, *Duke University;* Louis DiValentin, Aolin Ding, and Amin Hass, *Accenture;* Neil Zhenqiang Gong, Yiran Chen, and Hai "Helen" Li, *Duke University*

Fuzzing IV: Hardware and Firmware

SHiFT: Semi-hosted Fuzz Testing for Embedded Applications 5323
Alejandro Mera and Changming Liu, *Northeastern University;* Ruimin Sun, *Florida International University;* Engin Kirda and Long Lu, *Northeastern University*

Cascade: CPU Fuzzing via Intricate Program Generation 5341
Flavien Solt, Katharina Ceesay-Seitz, and Kaveh Razavi, *ETH Zurich*

MultiFuzz: A Multi-Stream Fuzzer For Testing Monolithic Firmware 5359
Michael Chesser, *The University of Adelaide and Data61 CSIRO, Cyber Security Cooperative Research Centre;* Surya Nepal, *Data61 CSIRO, Cyber Security Cooperative Research Centre;* Damith C. Ranasinghe, *The University of Adelaide*

WhisperFuzz: White-Box Fuzzing for Detecting and Locating Timing Vulnerabilities in Processors 5377
Pallavi Borkar, *Indian Institute of Technology Madras;* Chen Chen, *Texas A&M University;* Mohamadreza Rostami, *Technische Universität Darmstadt;* Nikhilesh Singh, *Indian Institute of Technology Madras;* Rahul Kande, *Texas A&M University;* Ahmad-Reza Sadeghi, *Technische Universität Darmstadt;* Chester Rebeiro, *Indian Institute of Technology Madras;* Jeyavijayan Rajendran, *Texas A&M University*

EL3XIR: Fuzzing COTS Secure Monitors 5395
Christian Lindenmeier, *FAU Erlangen-Nürnberg;* Mathias Payer and Marcel Busch, *EPFL*

Crypto IV: Position and Elections

GridSE: Towards Practical Secure Geographic Search via Prefix Symmetric Searchable Encryption 5413
Ruoyang Guo, Jiarui Li, and Shucheng Yu, *Stevens Institute of Technology*

Abuse-Resistant Location Tracking: Balancing Privacy and Safety in the Offline Finding Ecosystem 5431
Harry Eldridge, Gabrielle Beck, and Matthew Green, *Johns Hopkins University;* Nadia Heninger, *University of California, San Diego;* Abhishek Jain, *Johns Hopkins University*

Security and Privacy Analysis of Samsung's Crowd-Sourced Bluetooth Location Tracking System 5449
Tingfeng Yu, James Henderson, Alwen Tiu, and Thomas Haines, *School of Computing, The Australian National University*

The Decisive Power of Indecision: Low-Variance Risk-Limiting Audits and Election Contestation via Marginal Mark Recording. 5467
Benjamin Fuller, Rashmi Pai, and Alexander Russell, *University of Connecticut - Voting Technology Research Center*

ElectionGuard: a Cryptographic Toolkit to Enable Verifiable Elections 5485
Josh Benaloh and Michael Naehrig, *Microsoft Research;* Olivier Pereira, *Microsoft Research and UCLouvain;* Dan S. Wallach, *Rice University*

Measurement VI: Human Behavior and Security

A High Coverage Cybersecurity Scale Predictive of User Behavior 5503
Yukiko Sawaya, *KDDI Research Inc.;* Sarah Lu, *Massachusetts Institute of Technology;* Takamasa Isohara, *KDDI Research Inc.;* Mahmood Sharif, *Tel Aviv University*

Biosignal Authentication Considered Harmful Today 5521
Veena Krish, *Stony Brook University;* Nicola Paoletti and Milad Kazemi, *King's College London;* Scott Smolka and Amir Rahmati, *Stony Brook University*

GlobalConfusion: TrustZone Trusted Application 0-Days by Design 5537
Marcel Busch, Philipp Mao, and Mathias Payer, *EPFL*

PointerGuess: Targeted Password Guessing Model Using Pointer Mechanism 5555
Kedong Xiu and Ding Wang, *Nankai University*

Hardware Security IV: Firmware

FFXE: Dynamic Control Flow Graph Recovery for Embedded Firmware Binaries 5573
Ryan Tsang, Asmita, and Doreen Joseph, *University of California, Davis;* Soheil Salehi, *University of Arizona;* Prasant Mohapatra and Houman Homayoun, *University of California, Davis*

***CO3*: Concolic Co-execution for Firmware 5591**
Changming Liu, Alejandro Mera, and Engin Kirda, *Northeastern University;* Meng Xu, *University of Waterloo;* Long Lu, *Northeastern University*

Unveiling IoT Security in Reality: A Firmware-Centric Journey 5609
Nicolas Nino, *School of Computing, University of Georgia;* Ruibo Lu and Wei Zhou, *School of Cyber Science and Engineering, Huazhong University of Science and Technology;* Kyu Hyung Lee, *School of Computing, University of Georgia;* Ziming Zhao, *Khoury College of Computer Sciences, Northeastern University;* Le Guan, *School of Computing, University of Georgia*

Your Firmware Has Arrived: A Study of Firmware Update Vulnerabilities 5627
Yuhao Wu, Jinwen Wang, Yujie Wang, Shixuan Zhai, and Zihan Li, *Washington University in St. Louis;* Yi He, *Tsinghua University;* Kun Sun, *George Mason University;* Qi Li, *Tsinghua University;* Ning Zhang, *Washington University in St. Louis*

Mobile Privacy

Abandon All Hope Ye Who Enter Here: A Dynamic, Longitudinal Investigation of Android's Data Safety Section 5645
Ioannis Arkalakis, Michalis Diamantaris, Serafeim Moustakas, and Sotiris Ioannidis, *Technical University of Crete;* Jason Polakis, *University of Illinois Chicago;* Panagiotis Ilia, *Cyprus University of Technology*

***iHunter*: Hunting Privacy Violations at Scale in the Software Supply Chain on iOS 5663**
Dexin Liu, *Peking University and Alibaba Group;* Yue Xiao and Chaoqi Zhang, *Indiana University Bloomington;* Kaitao Xie and Xiaolong Bai, *Alibaba Group;* Shikun Zhang, *Peking University;* Luyi Xing, *Indiana University Bloomington*

Is It a Trap? A Large-scale Empirical Study And Comprehensive Assessment of Online Automated Privacy Policy Generators for Mobile Apps 5681
Shidong Pan and Dawen Zhang, *CSIRO's Data61 & Australian National University;* Mark Staples, *CSIRO's Data61;* Zhenchang Xing, *CSIRO's Data61 & Australian National University;* Jieshan Chen, Xiwei Xu, and Thong Hoang, *CSIRO's Data61*

A New Hope: Contextual Privacy Policies for Mobile Applications and An Approach Toward Automated Generation 5699
Shidong Pan and Zhen Tao, *CSIRO's Data61 and Australian National University;* Thong Hoang, *CSIRO's Data61;* Dawen Zhang, *CSIRO's Data61 and Australian National University;* Tianshi Li, *Northeastern University;* Zhenchang Xing, *CSIRO's Data61 and Australian National University;* Xiwei Xu, Mark Staples, and Thierry Rakotoarivelo, *CSIRO's Data61;* David Lo, *Singapore Management University*

Network Security IV: Infrastructure

CDN Cannon: Exploiting CDN Back-to-Origin Strategies for Amplification Attacks 5717
Ziyu Lin, *Fuzhou University and Tsinghua University;* Zhiwei Lin, *Sichuan University and Tsinghua University;* Ximeng Liu, *Fuzhou University;* Jianjun Chen and Run Guo, *Tsinghua University;* Cheng Chen and Shaodong Xiao, *Fuzhou University*

You Can Obfuscate, but You Cannot Hide: CrossPoint Attacks against Network Topology Obfuscation 5735
Xuanbo Huang, Kaiping Xue, Lutong Chen, and Mingrui Ai, *University of Science and Technology of China;* Huancheng Zhou, *Texas A&M University;* Bo Luo, *The University of Kansas;* Guofei Gu, *Texas A&M University;* Qibin Sun, *University of Science and Technology of China*

Cross the Zone: Toward a Covert Domain Hijacking via Shared DNS Infrastructure. 5751
Yunyi Zhang, *National University of Defense Technology; Tsinghua University;* Mingming Zhang, *Zhongguancun Laboratory;* Baojun Liu, *Tsinghua University; Zhongguancun Laboratory;* Zhan Liu and Jia Zhang, *Tsinghua University;* Haixin Duan, *Tsinghua University; Zhongguancun Laboratory;* Min Zhang, Fan Shi, and Chengxi Xu, *National University of Defense Technology*

CAMP: Compositional Amplification Attacks against DNS 5769
Huayi Duan, Marco Bearzi, Jodok Vieli, David Basin, Adrian Perrig, and Si Liu, *ETH Zürich;* Bernhard Tellenbach, *Armasuisse*

LLM III: Abuse

Moderating Illicit Online Image Promotion for Unsafe User Generated Content Games Using Large Vision-Language Models 5787
Keyan Guo, Ayush Utkarsh, Wenbo Ding, and Isabelle Ondracek, *University at Buffalo;* Ziming Zhao, *Northeastern University;* Guo Freeman, *Clemson University;* Nishant Vishwamitra, *The University of Texas at San Antonio;* Hongxin Hu, *University at Buffalo*

Deciphering Textual Authenticity: A Generalized Strategy through the Lens of Large Language Semantics for Detecting Human vs. Machine-Generated Text. 5805
Mazal Bethany, *The University of Texas at San Antonio and Secure AI and Autonomy Lab;* Brandon Wherry, *The University of Texas at San Antonio, Secure AI and Autonomy Lab, and Peraton Labs;* Emet Bethany, *The University of Texas at San Antonio and Secure AI and Autonomy Lab;* Nishant Vishwamitra and Anthony Rios, *The University of Texas at San Antonio;* Peyman Najafirad, *The University of Texas at San Antonio and Secure AI and Autonomy Lab*

Prompt Stealing Attacks Against Text-to-Image Generation Models. 5823
Xinyue Shen, Yiting Qu, Michael Backes, and Yang Zhang, *CISPA Helmholtz Center for Information Security*

Quantifying Privacy Risks of Prompts in Visual Prompt Learning 5841
Yixin Wu, Rui Wen, and Michael Backes, *CISPA Helmholtz Center for Information Security;* Pascal Berrang, *University of Birmingham;* Mathias Humbert, *University of Lausanne;* Yun Shen, *Netapp;* Yang Zhang, *CISPA Helmholtz Center for Information Security*

Security Analysis IV: OS

Pandawan: Quantifying Progress in Linux-based Firmware Rehosting 5859
Ioannis Angelakopoulos, Gianluca Stringhini, and Manuel Egele, *Boston University*

DeepType: Refining Indirect Call Targets with Strong Multi-layer Type Analysis 5877
Tianrou Xia, Hong Hu, and Dinghao Wu, *The Pennsylvania State University*

Improving Indirect-Call Analysis in LLVM with Type and Data-Flow Co-Analysis 5895
Dinghao Liu and Shouling Ji, *Zhejiang University;* Kangjie Lu, *University of Minnesota;* Qinming He, *Zhejiang University*

ChainReactor: Automated Privilege Escalation Chain Discovery via AI Planning 5913
Giulio De Pasquale, *King's College London and University College London;* Ilya Grishchenko, *University of California, Santa Barbara;* Riccardo Iesari, *Vrije Universiteit Amsterdam;* Gabriel Pizarro, *University of California, Santa Barbara;* Lorenzo Cavallaro, *University College London;* Christopher Kruegel and Giovanni Vigna, *University of California, Santa Barbara*

Crypto V: Private Information Retrieval

VeriSimplePIR: Verifiability in SimplePIR at No Online Cost for Honest Servers 5931
Leo de Castro, *MIT;* Keewoo Lee, *Seoul National University*

Batch PIR and Labeled PSI with Oblivious Ciphertext Compression 5949
Alexander Bienstock, *New York University;* Sarvar Patel and Joon Young Seo, *Google;* Kevin Yeo, *Google and Columbia University*

Single Pass Client-Preprocessing Private Information Retrieval 5967
Arthur Lazzaretti and Charalampos Papamanthou, *Yale University*

YPIR: High-Throughput Single-Server PIR with Silent Preprocessing 5985
Samir Jordan Menon, *Blyss;* David J. Wu, *UT Austin*

User Studies VII: Policies and Best Practices III

Trust Me *If You Can* – How Usable Is Trusted Types In Practice? 6003
Sebastian Roth, *TU Wien;* Lea Gröber, *CISPA Helmholtz Center for Information Security;* Philipp Baus, *Saarland University;* Katharina Krombholz and Ben Stock, *CISPA Helmholtz Center for Information Security*

"I just hated it and I want my money back": Data-driven Understanding of Mobile VPN Service Switching Preferences in The Wild 6021
Rohit Raj, Mridul Newar, and Mainack Mondal, *Indian Institute of Technology, Kharagpur*

I Experienced More than 10 DeFi Scams: On DeFi Users' Perception of Security Breaches and Countermeasures . . 6039
Mingyi Liu, *Georgia Institute of Technology;* Jun Ho Huh, *Samsung Research;* HyungSeok Han, Jaehyuk Lee, Jihae Ahn, and Frank Li, *Georgia Institute of Technology;* Hyoungshick Kim, *Sungkyunkwan University;* Taesoo Kim, *Georgia Institute of Technology*

Towards Privacy and Security in Private Clouds: A Representative Survey on the Prevalence of Private Hosting and Administrator Characteristics 6057
Lea Gröber, *CISPA Helmholtz Center for Information Security and Saarland University;* Simon Lenau and Rebecca Weil, *CISPA Helmholtz Center for Information Security;* Elena Groben, *Saarland University;* Michael Schilling and Katharina Krombholz, *CISPA Helmholtz Center for Information Security*

Wireless Security II: Sky and Space

Wireless Signal Injection Attacks on VSAT Satellite Modems. 6075
Robin Bisping, *ETH Zurich;* Johannes Willbold, *Ruhr University Bochum;* Martin Strohmeier and Vincent Lenders, *Cyber-Defence Campus, armasuisse*

Orbital Trust and Privacy: SoK on PKI and Location Privacy Challenges in Space Networks 6093
David Koisser, *Sanctuary;* Richard Mitev, *Technische Universität Darmstadt;* Nikita Yadav, *Indian Institute of Science, Bangalore;* Franziska Vollmer and Ahmad-Reza Sadeghi, *Technische Universität Darmstadt*

RECORD: A RECeption-Only Region Determination Attack on LEO Satellite Users 6113
Eric Jedermann, *RPTU Kaiserslautern-Landau;* Martin Strohmeier and Vincent Lenders, *armasuisse;* Jens Schmitt, *RPTU Kaiserslautern-Landau*

On a Collision Course: Unveiling Wireless Attacks to the Aircraft Traffic Collision Avoidance System (TCAS) . . .6131
Giacomo Longo, *DIBRIS, University of Genova;* Martin Strohmeier, *Cyber-Defence Campus, armasuisse S + T;* Enrico Russo, *DIBRIS, University of Genova;* Alessio Merlo, *CASD, School of Advanced Defense Studies;* Vincent Lenders, *Cyber-Defence Campus, armasuisse S + T*

System Security IV: Multithreading

LR-Miner: Static Race Detection in OS Kernels by Mining Locking Rules. 6149
Tuo Li, *Tsinghua University;* Jia-Ju Bai and Gui-Dong Han, *Beihang University;* Shi-Min Hu, *Tsinghua University*

When Threads Meet Interrupts: Effective Static Detection of Interrupt-Based Deadlocks in Linux 6167
Chengfeng Ye, Yuandao Cai, and Charles Zhang, *The Hong Kong University of Science and Technology*

GhostRace: Exploiting and Mitigating Speculative Race Conditions 6185
Hany Ragab, *Vrije Universiteit Amsterdam;* Andrea Mambretti and Anil Kurmus, *IBM Research Europe - Zurich;* Cristiano Giuffrida, *Vrije Universiteit Amsterdam*

CARDSHARK: Understanding and Stablizing Linux Kernel Concurrency Bugs Against the Odds 6203
Tianshuo Han, Xiaorui Gong, and Jian Liu, *{CAS-KLONAT, BKLONSPT}, Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences*

Blockchain II

zkCross: A Novel Architecture for Cross-Chain Privacy-Preserving Auditing 6219
Yihao Guo, Minghui Xu, Xiuzhen Cheng, and Dongxiao Yu, *Shandong University;* Wangjie Qiu, *Beihang University;* Gang Qu, *University of Maryland;* Weibing Wang and Mingming Song, *Cloud Inspur Information Technology Co., Ltd.*

Pixel+ and Pixel++: Compact and Efficient Forward-Secure Multi-Signatures for PoS Blockchain Consensus . . . 6237
Jianghong Wei, *State Key Laboratory of Integrated Service Networks (ISN), Xidian University, and State Key Laboratory of Mathematical Engineering and Advanced Computing;* Guohua Tian, *State Key Laboratory of Integrated Service Networks (ISN), Xidian University;* Ding Wang, *College of Cyber Science, Nankai University;* Fuchun Guo and Willy Susilo, *School of Computing and Information Technology, University of Wollongong;* Xiaofeng Chen, *State Key Laboratory of Integrated Service Networks (ISN), Xidian University*

Max Attestation Matters: Making Honest Parties Lose Their Incentives in Ethereum PoS 6255
Mingfei Zhang, *Shandong University;* Rujia Li and Sisi Duan, *Tsinghua University*

Sprints: Intermittent Blockchain PoW Mining 6273
Michael Mirkin, *Technion;* Lulu Zhou, *Yale University;* Ittay Eyal, *Technion;* Fan Zhang, *Yale University*

Autonomous and Automatic Systems

A First Physical-World Trajectory Prediction Attack via LiDAR-induced Deceptions in Autonomous Driving . . . 6291
Yang Lou, *City University of Hong Kong;* Yi Zhu, *State University of New York at Buffalo;* Qun Song, *Delft University of Technology;* Rui Tan, *Nanyang Technological University;* Chunming Qiao, *State University of New York at Buffalo;* Wei-Bin Lee, *Information Security Center, Hon Hai Research Institute, and Feng Chia University;* Jianping Wang, *City University of Hong Kong*

On Data Fabrication in Collaborative Vehicular Perception: Attacks and Countermeasures 6309
Qingzhao Zhang, Shuowei Jin, Ruiyang Zhu, Jiachen Sun, and Xumiao Zhang, *University of Michigan;* Qi Alfred Chen, *University of California, Irvine;* Z. Morley Mao, *University of Michigan and Google*

VOGUES: Validation of Object Guise using Estimated Components 6327
Raymond Muller, *Purdue University;* Yanmao Man and Ming Li, *University of Arizona;* Ryan Gerdes, *Virginia Tech;* Jonathan Petit, *Qualcomm;* Z. Berkay Celik, *Purdue University*

Adversary is on the Road: Attacks on Visual SLAM using Unnoticeable Adversarial Patch 6345
Baodong Chen, *The Ohio State University;* Wei Wang and Pascal Sikorski, *Saint Louis University;* Ting Zhu, *The Ohio State University*

Crypto VI: Security Analysis

Cryptographic Analysis of Delta Chat 6363
Yuanming Song, Lenka Mareková, and Kenneth G. Paterson, *ETH Zurich*

ENG25519: Faster TLS 1.3 handshake using optimized X25519 and Ed25519 6381
Jipeng Zhang, *CCST, Nanjing University of Aeronautics and Astronautics;* Junhao Huang, *Guangdong Provincial Key Laboratory IRADS, BNU-HKBU United International College; Hong Kong Baptist University;* Lirui Zhao, *CCST, Nanjing University of Aeronautics and Astronautics;* Donglong Chen, *Guangdong Provincial Key Laboratory IRADS, BNU-HKBU United International College;* Çetin Kaya Koç, *CCST, Nanjing University of Aeronautics and Astronautics; Iğdır University; University of California Santa Barbara*

Formal Security Analysis of Widevine through the W3C EME Standard 6399
Stéphanie Delaune and Joseph Lallemand, *Univ Rennes, CNRS, IRISA, France;* Gwendal Patat, *Fraunhofer SIT | ATHENE, Germany;* Florian Roudot and Mohamed Sabt, *Univ Rennes, CNRS, IRISA, France*

Length Leakage in Oblivious Data Access Mechanisms. 6417
Grace Jia, *Yale University;* Rachit Agarwal, *Cornell University;* Anurag Khandelwal, *Yale University*

Crypto VII: Private Set Operations

Unbalanced Circuit-PSI from Oblivious Key-Value Retrieval 6435
Meng Hao, *Nanyang Technological University;* Weiran Liu and Liqiang Peng, *Alibaba Group;* Hongwei Li, *Peng Cheng Laboratory;* Cong Zhang, *Institute for Advanced Study, BNRist, Tsinghua University;* Hanxiao Chen and Tianwei Zhang, *Nanyang Technological University*

PEPSI: Practically Efficient Private Set Intersection in the Unbalanced Setting 6453
Rasoul Akhavan Mahdavi, Nils Lukas, Faezeh Ebrahimianghazani, and Thomas Humphries, *University of Waterloo;* Bailey Kacsmar, *University of Alberta;* John Premkumar and Xinda Li, *University of Waterloo;* Simon Oya, *University of British Columbia;* Ehsan Amjadian, *University of Waterloo and Royal Bank of Canada;* Florian Kerschbaum, *University of Waterloo*

Scalable Private Set Union, with Stronger Security 6471
Yanxue Jia, *Purdue University;* Shi-Feng Sun, *Shanghai Jiao Tong University;* Hong-Sheng Zhou, *Virginia Commonwealth University;* Dawu Gu, *Shanghai Jiao Tong University*

O-Ring and K-Star: Efficient Multi-party Private Set Intersection 6489
Mingli Wu, *The University of Hong Kong;* Tsz Hon Yuen, *Monash University;* Kwan Yin Chan, *The University of Hong Kong*

Social Issues IV

Being Transparent is Merely the Beginning: Enforcing Purpose Limitation with Polynomial Approximation . . . 6507
Shuofeng Liu and Zihan Wang, *The University of Queensland and CSIRO's Data61;* Minhui Xue, *CSIRO's Data61;* Long Wang and Yuanchao Zhang, *Information Security Department, Ant Group, MYBank;* Guangdong Bai, *The University of Queensland*

DVSorder: Ballot Randomization Flaws Threaten Voter Privacy 6525
Braden L. Crimmins and Dhanya Y. Narayanan, *University of Michigan;* Drew Springall, *Auburn University;* J. Alex Halderman, *University of Michigan*

Navigating the Privacy Compliance Maze: Understanding Risks with Privacy-Configurable Mobile SDKs. 6543
Yifan Zhang, *Indiana University Bloomington;* Zhaojie Hu and Xueqiang Wang, *University of Central Florida;* Yuhui Hong, *Indiana University Bloomington;* Yuhong Nan, *Sun Yat-sen University;* XiaoFeng Wang, *Indiana University Bloomington;* Jiatao Cheng, *Sun Yat-sen University;* Luyi Xing, *Indiana University Bloomington*

Enabling Developers, Protecting Users: Investigating Harassment and Safety in VR 6561
Abhinaya S.B., Aafaq Sabir, and Anupam Das, *North Carolina State University*

IoT and CPS

Demystifying the Security Implications in IoT Device Rental Services 6579
Yi He and Yunchao Guan, *Tsinghua University;* Ruoyu Lun, *China National Digital Switching System Engineering and Technological Research Center;* Shangru Song and Zhihao Guo, *Tsinghua University;* Jianwei Zhuge and Jianjun Chen, *Tsinghua University and Zhongguancun Laboratory;* Qiang Wei and Zehui Wu, *China National Digital Switching System Engineering and Technological Research Center;* Miao Yu and Hetian Shi, *Tsinghua University;* Qi Li, *Tsinghua University and Zhongguancun Laboratory*

SAIN: Improving ICS Attack Detection Sensitivity via State-Aware Invariants 6597
Syed Ghazanfar Abbas, Muslum Ozgur Ozmen, Abdulellah Alsaheel, Arslan Khan, Z. Berkay Celik, and Dongyan Xu, *Purdue University*

Opportunistic Data Flow Integrity for Real-time Cyber-physical Systems Using Worst Case Execution Time Reservation 6615
Yujie Wang, Ao Li, Jinwen Wang, Sanjoy Baruah, and Ning Zhang, *Washington University in St. Louis*

On Bridging the Gap between Control Flow Integrity and Attestation Schemes 6633
Mahmoud Ammar, Ahmed Abdelraoof, and Silviu Vlasceanu, *Huawei Research, Germany*

Crypto VIII: Side Channel

Windows into the Past: Exploiting Legacy Crypto in Modern OS's Kerberos Implementation 6651
Michal Shagam and Eyal Ronen, *Tel Aviv University*

Divide and Surrender: Exploiting Variable Division Instruction Timing in HQC Key Recovery Attacks 6669
Robin Leander Schröder, *Fraunhofer SIT, Darmstadt, Germany and Fraunhofer Austria, Vienna, Austria;* Stefan Gast, *Graz University of Technology, Austria;* Qian Guo, *Lund University, Sweden*

With Great Power Come Great Side Channels: Statistical Timing Side-Channel Analyses with Bounded Type-1 Errors 6687
Martin Dunsche, Marcel Maehren, and Nurullah Erinola, *Ruhr University Bochum;* Robert Merget, *Technology Innovation Institute;* Nicolai Bissantz, *Ruhr University Bochum;* Juraj Somorovsky, *Paderborn University;* Jörg Schwenk, *Ruhr University Bochum*

"These results must be false": A usability evaluation of constant-time analysis tools. 6705
Marcel Fourné, *Paderborn University and MPI-SP;* Daniel De Almeida Braga, *Rennes University, CNRS, IRISA;* Jan Jancar, *Masaryk University;* Mohamed Sabt, *Rennes University, CNRS, IRISA;* Peter Schwabe, *MPI-SP and Radboud University;* Gilles Barthe, *MPI-SP and IMDEA Software Institute;* Pierre-Alain Fouque, *Rennes University, CNRS, IRISA;* Yasemin Acar, *Paderborn University and George Washington University*

Web Security III: XSS and PHP

Dancer in the Dark: Synthesizing and Evaluating Polyglots for Blind Cross-Site Scripting 6723
Robin Kirchner, *Technische Universität Braunschweig;* Jonas Möller, *Technische Universität Berlin;* Marius Musch and David Klein, *Technische Universität Braunschweig;* Konrad Rieck, *Technische Universität Berlin;* Martin Johns, *Technische Universität Braunschweig*

Spider-Scents: Grey-box Database-aware Web Scanning for Stored XSS 6741
Eric Olsson and Benjamin Eriksson, *Chalmers University of Technology;* Adam Doupé, *Arizona State University;* Andrei Sabelfeld, *Chalmers University of Technology*

Argus: All your (PHP) Injection-sinks are belong to us. 6759
Rasoul Jahanshahi and Manuel Egele, *Boston University*

SSRF vs. Developers: A Study of SSRF-Defenses in PHP Applications 6777
Malte Wessels and Simon Koch, *Technische Universität Braunschweig;* Giancarlo Pellegrino, *CISPA Helmholtz Center for Information Security;* Martin Johns, *Technische Universität Braunschweig*

ML X: Privacy Inference II

How Does a Deep Learning Model Architecture Impact Its Privacy? A Comprehensive Study of Privacy Attacks on CNNs and Transformers. 6795
Guangsheng Zhang, Bo Liu, Huan Tian, and Tianqing Zhu, *University of Technology Sydney;* Ming Ding, *Data 61, Australia;* Wanlei Zhou, *City University of Macau*

Reconstructing training data from document understanding models **6813**
Jérémie Dentan, *Crédit Agricole SA and École Polytechnique, IP Paris;* Arnaud Paran and Aymen Shabou, *Crédit Agricole SA*

Privacy Side Channels in Machine Learning Systems **6831**
Edoardo Debenedetti, *ETH Zurich;* Giorgio Severi, *Northeastern University;* Nicholas Carlini, Christopher A. Choquette-Choo, Matthew Jagielski, and Milad Nasr, *Google DeepMind;* Eric Wallace, *UC Berkeley;* Florian Tramèr, *ETH Zurich*

FaceObfuscator: Defending Deep Learning-based Privacy Attacks with Gradient Descent-resistant Features in Face Recognition **6849**
Shuaifan Jin, He Wang, and Zhibo Wang, *Zhejiang University;* Feng Xiao, *Palo Alto Networks;* Jiahui Hu, *Zhejiang University;* Yuan He and Wenwen Zhang, *Alibaba Group;* Zhongjie Ba, Weijie Fang, Shuhong Yuan, and Kui Ren, *Zhejiang University*

Security Analysis V: ML

Hijacking Attacks against Neural Network by Analyzing Training Data **6867**
Yunjie Ge, Qian Wang, and Huayang Huang, *Wuhan University;* Qi Li, *Tsinghua University; BNRist;* Cong Wang, *City University of Hong Kong;* Chao Shen, *Xi'an Jiaotong University;* Lingchen Zhao, *Wuhan University;* Peipei Jiang, *Wuhan University; City University of Hong Kong;* Zheng Fang and Shenyi Zhang, *Wuhan University*

False Claims against Model Ownership Resolution **6885**
Jian Liu and Rui Zhang, *Zhejiang University;* Sebastian Szyller, *Intel Labs & Aalto University;* Kui Ren, *Zhejiang University;* N. Asokan, *University of Waterloo & Aalto University*

Landscape More Secure Than Portrait? Zooming Into the Directionality of Digital Images With Security Implications **6903**
Benedikt Lorch and Rainer Böhme, *University of Innsbruck*

Information Flow Control in Machine Learning through Modular Model Architecture **6921**
Trishita Tiwari, *Cornell University;* Suchin Gururangan, *University of Washington;* Chuan Guo, *FAIR at Meta;* Weizhe Hua, *Google DeepMind;* Sanjay Kariyappa, *Georgia Institute of Technology;* Udit Gupta, *Cornell University;* Wenjie Xiong, *Virginia Tech;* Kiwan Maeng, *Pennsylvania State University;* Hsien-Hsin S. Lee, *Intel;* G. Edward Suh, *NVIDIA/Cornell University*

Cryptographic Protocols III

POPSTAR: Lightweight Threshold Reporting with Reduced Leakage **6939**
Hanjun Li, Sela Navot, and Stefano Tessaro, *University of Washington*

Privacy-Preserving Data Aggregation with Public Verifiability Against Internal Adversaries **6957**
Marco Palazzo and Florine W. Dekker, *Cyber Security Group, Delft University of Technology;* Alessandro Brighente, *SPRITZ Security and Privacy Research Group, Università di Padova;* Mauro Conti, *SPRITZ Security and Privacy Research Group, Università di Padova & Cyber Security Group, Delft University of Technology;* Zekeriya Erkin, *Cyber Security Group, Delft University of Technology*

PINE: Efficient Verification of a Euclidean Norm Bound of a Secret-Shared Vector **6975**
Guy N. Rothblum, *Apple;* Eran Omri, *Ariel University and Ariel Cyber Innovation Center;* Junye Chen and Kunal Talwar, *Apple*

DaCapo: Automatic Bootstrapping Management for Efficient Fully Homomorphic Encryption **6993**
Seonyoung Cheon, Yongwoo Lee, Dongkwan Kim, and Ju Min Lee, *Yonsei University;* Sunchul Jung and Taekyung Kim, *CryptoLab. Inc.;* Dongyoon Lee, *Stony Brook University;* Hanjun Kim, *Yonsei University*

Measurement VII: Auditing and Best Practices II

SoK (or SoLK?): On the Quantitative Study of Sociodemographic Factors and Computer Security Behaviors **7011**
Miranda Wei, *University of Washington;* Jaron Mink, *University of Illinois at Urbana-Champaign;* Yael Eiger and Tadayoshi Kohno, *University of Washington;* Elissa M. Redmiles, *Georgetown University;* Franziska Roesner, *University of Washington*

IoT Market Dynamics: An Analysis of Device Sales, Security and Privacy Signals, and their Interactions **7031**
Swaathi Vetrivel, Brennen Bouwmeester, Michel van Eeten, and Carlos H. Gañán, *Delft University of Technology*

The Unpatchables: Why Municipalities Persist in Running Vulnerable Hosts 7049
Aksel Ethembabaoglu, Rolf van Wegberg, Yury Zhauniarovich, and Michel van Eeten, *Delft University of Technology*

Hardware Security V: Embedded

Leveraging Semantic Relations in Code and Data to Enhance Taint Analysis of Embedded Systems 7067
Jiaxu Zhao, *Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences; Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences; Beijing Key Laboratory of Network Security and Protection Technology;* Yuekang Li, *The University of New South Wales;* Yanyan Zou, Zhaohui Liang, Yang Xiao, Yeting Li, Bingwei Peng, Nanyu Zhong, and Xinyi Wang, *Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences; Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences; Beijing Key Laboratory of Network Security and Protection Technology;* Wei Wang, *Institute of Information Engineering, Chinese Academy of Sciences; Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences; Beijing Key Laboratory of Network Security and Protection Technology;* Wei Huo, *Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences; Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences; Beijing Key Laboratory of Network Security and Protection Technology*

A Friend's Eye is A Good Mirror: Synthesizing MCU Peripheral Models from Peripheral Drivers 7085
Chongqing Lei and Zhen Ling, *Southeast University;* Yue Zhang, *Drexel University;* Yan Yang and Junzhou Luo, *Southeast University;* Xinwen Fu, *University of Massachusetts Lowell*

SoK: Security of Programmable Logic Controllers 7103
Efrén López-Morales, *Texas A&M University-Corpus Christi;* Ulysse Planta, *CISPA Helmholtz Center for Information Security;* Carlos Rubio-Medrano, *Texas A&M University-Corpus Christi;* Ali Abbasi, *CISPA Helmholtz Center for Information Security;* Alvaro A. Cardenas, *University of California, Santa Cruz*

Operation Mango: Scalable Discovery of Taint-Style Vulnerabilities in Binary Firmware Services 7123
Wil Gibbs, Arvind S Raj, Jayakrishna Menon Vadayath, Hui Jun Tay, Jennifer Miller, Akshay Ajayan, Zion Leonahenahe Basque, Audrey Dutcher, and Fangzhou Dong, *Arizona State University;* Xavier Maso, *unaffiliated;* Giovanni Vigna and Christopher Kruegel, *UC Santa Barbara;* Adam Doupé, Yan Shoshitaishvili, and Ruoyu Wang, *Arizona State University*

System Security V: Memory II

Scavy: Automated Discovery of Memory Corruption Targets in Linux Kernel for Privilege Escalation 7141
Erin Avllazagaj, Yonghwi Kwon, and Tudor Dumitraș, *University of Maryland*

Voodoo: Memory Tagging, Authenticated Encryption, and Error Correction through MAGIC 7159
Lukas Lamster, Martin Unterguggenberger, David Schrammel, and Stefan Mangard, *Graz University of Technology*

ShadowBound: Efficient Heap Memory Protection Through Advanced Metadata Management and Customized Compiler Optimization. 7177
Zheng Yu, Ganxiang Yang, and Xinyu Xing, *Northwestern University*

OptiSan: Using Multiple Spatial Error Defenses to Optimize Stack Memory Protection within a Budget 7195
Rahul George, *University of California, Riverside;* Mingming Chen and Kaiming Huang, *The Pennsylvania State University;* Zhiyun Qian, *University of California, Riverside;* Thomas La Porta, *The Pennsylvania State University;* Trent Jaeger, *University of California, Riverside*

User Studies VIII: Cryptography

The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts 7213
Konstantin Fischer, *Ruhr University Bochum;* Ivana Trummová, *Czech Technical University in Prague;* Phillip Gajland, *Ruhr University Bochum and Max Planck Institute for Security and Privacy;* Yasemin Acar, *Paderborn University and The George Washington University;* Sascha Fahl, *CISPA - Helmholtz-Center for Information Security;* Angela Sasse, *Ruhr University Bochum*

Why Aren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication 7231
Leona Lassak, *Ruhr University Bochum;* Elleen Pan and Blase Ur, *University of Chicago;* Maximilian Golla, *CISPA Helmholtz Center for Information Security*

"You have to read 50 different RFCs that contradict each other": An Interview Study on the Experiences of Implementing Cryptographic Standards 7249
Nicolas Huaman and Jacques Suray, *Leibniz University Hannover;* Jan H. Klemmer, *CISPA Helmholtz Center for Information Security;* Marcel Fourné, *Paderborn University;* Sabrina Amft, *CISPA Helmholtz Center for Information Security;* Ivana Trummová, *Czech Technical University in Prague;* Yasemin Acar, *Paderborn University & The George Washington University;* Sascha Fahl, *CISPA Helmholtz Center for Information Security*

A Mixed-Methods Study on User Experiences and Challenges of Recovery Codes for an End-to-End Encrypted Service 7267
Sandra Höltervennhoff, *Leibniz University Hannover;* Noah Wöhler, *CISPA Helmholtz Center for Information Security;* Arne Möhle, *Tutao GmbH;* Marten Oltrogge, *CISPA Helmholtz Center for Information Security;* Yasemin Acar, *Paderborn University and The George Washington University;* Oliver Wiese and Sascha Fahl, *CISPA Helmholtz Center for Information Security*

ML XI: Physical Adversarial Attacks

Devil in the Room: Triggering Audio Backdoors in the Physical World. 7285
Meng Chen, *Zhejiang University;* Xiangyu Xu, *Southeast University;* Li Lu, Zhongjie Ba, Feng Lin, and Kui Ren, *Zhejiang University*

FraudWhistler: A Resilient, Robust and Plug-and-play Adversarial Example Detection Method for Speaker Recognition 7303
Kun Wang, *Zhejiang University;* Xiangyu Xu, *Southeast University;* Li Lu, Zhongjie Ba, Feng Lin, and Kui Ren, *Zhejiang University*

π-Jack: Physical-World Adversarial Attack on Monocular Depth Estimation with Perspective Hijacking 7321
Tianyue Zheng, *Southern University of Science and Technology;* Jingzhi Hu and Rui Tan, *Nanyang Technological University;* Yinqian Zhang, *Southern University of Science and Technology;* Ying He and Jun Luo, *Nanyang Technological University*

AE-Morpher: Improve Physical Robustness of Adversarial Objects against LiDAR-based Detectors via Object Reconstruction 7339
Shenchen Zhu, *Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China;* Yue Zhao, *Institute of Information Engineering, Chinese Academy of Sciences, China;* Kai Chen, *Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China;* Bo Wang, *Huawei Technologies Co., Ltd.;* Hualong Ma and Cheng'an Wei, *Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China*

Software Security + ML 2

EaTVul: ChatGPT-based Evasion Attack Against Software Vulnerability Detection. 7357
Shigang Liu, *CSIRO's Data61 and Swinburne University of Technology;* Di Cao, *Swinburne University of Technology;* Junae Kim, Tamas Abraham, and Paul Montague, *DST Group, Australia;* Seyit Camtepe, *CSIRO's Data61;* Jun Zhang and Yang Xiang, *Swinburne University of Technology*

FVD-DPM: Fine-grained Vulnerability Detection via Conditional Diffusion Probabilistic Models 7375
Miaomiao Shao and Yuxin Ding, *Harbin Institute of Technology, Shenzhen*

A Wolf in Sheep's Clothing: Practical Black-box Adversarial Attacks for Evading Learning-based Windows Malware Detection in the Wild 7393
Xiang Ling, *Intelligent Software Research Center, Institute of Software, Chinese Academy of Sciences; Key Laboratory of System Software (Chinese Academy of Sciences); State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences;* Zhiyu Wu, *Zhejiang University;* Bin Wang, *Zhejiang Key Laboratory of Artificial Intelligence of Things (AIoT) Network and Data Security; Hangzhou Research Institute, Xidian University;* Wei Deng, *Zhejiang University;* Jingzheng Wu, *Intelligent Software Research Center, Institute of Software, Chinese Academy of Sciences; Key Laboratory of System Software (Chinese Academy of Sciences); State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences;* Shouling Ji, *Zhejiang University;* Tianyue Luo, *Intelligent Software Research Center, Institute of Software, Chinese Academy of Sciences;* Yanjun Wu, *Intelligent Software Research Center, Institute of Software, Chinese Academy of Sciences; Key Laboratory of System Software (Chinese Academy of Sciences); State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences*

Crypto IX: Attacks

Leakage-Abuse Attacks Against Structured Encryption for SQL 7411
Alexander Hoover, *University of Chicago;* Ruth Ng, Daren Khu, Yao'An Li, Joelle Lim, and Derrick Ng, *DSO National Laboratories;* Jed Lim, *NUS High School of Mathematics and Science;* Yiyang Song, *Raffles Institution*

RADIUS/UDP Considered Harmful. 7429
Sharon Goldberg, *Cloudflare;* Miro Haller and Nadia Heninger, *UC San Diego;* Mike Milano, *BastionZero;* Dan Shumow, *Microsoft Research;* Marc Stevens, *Centrum Wiskunde & Informatica;* Adam Suhl, *UC San Diego*

Key Recovery Attacks on Approximate Homomorphic Encryption with Non-Worst-Case Noise Flooding Countermeasures 7447
Qian Guo and Denis Nabokov, *Lund University;* Elias Suvanto, *ENS Lyon;* Thomas Johansson, *Lund University*

Terrapin Attack: Breaking SSH Channel Integrity By Sequence Number Manipulation 7463
Fabian Bäumer, Marcus Brinkmann, and Jörg Schwenk, *Ruhr University Bochum*