34th USENIX Security Symposium (USENIX Security'25)

Seattle, Washington, USA
13-15 August 2025

Volume 1 of 11

ISBN: 979-8-3313-2589-3

Printed from e-media with permission by:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571

Some format issues inherent in the e-media version may also appear in this print version.

Copyright© (2025) by Usenix Association
All rights reserved.

Printed with permission by Curran Associates, Inc. (2025)

For permission requests, please contact Usenix Association
at the address below.

Usenix Association
2560 Ninth Street, Suite 215
Berkeley, California, 94710

https://www.usenix.org/

Additional copies of this publication are available from:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: 845-758-0400
Fax: 845-758-2633
Email: curran@proceedings.com
Web: www.proceedings.com

34th USENIX Security Symposium

August 13–15, 2025
Seattle, WA, USA

Wednesday, August 13

Social Issues and Usable Security and Privacy

Analyzing the AI Nudification Application Ecosystem 1
Cassidy Gibson and Daniel Olszewski, *University of Florida;* Natalie Grace Brigham, *University of Washington;* Anna Crowder, Kevin R. B. Butler, and Patrick Traynor, *University of Florida;* Elissa M. Redmiles, *Georgetown University;* Tadayoshi Kohno, *University of Washington*

Easy As *Child's Play*: An Empirical Study on Age Verification of Adult-Oriented Android Apps 21
Yifan Yao, Shawn McCollum, Zhibo Sun, and Yue Zhang, *Drexel University*

Abusability of Automation Apps in Intimate Partner Violence 41
Shirley Zhang, *University of Wisconsin–Madison;* Paul Chung, *University of California, San Diego;* Jacob Vervelde, Nishant Korapati, Rahul Chatterjee, and Kassem Fawaz, *University of Wisconsin–Madison*

Malicious LLM-Based Conversational AI Makes Users Reveal Personal Information 61
Xiao Zhan, *King's College London;* Juan Carlos Carrillo, *VRAIN, Universitat Politècnica de València;* William Seymour, *King's College London;* Jose Such, *King's College London and VRAIN, Universitat Politècnica de València*

An Industry Interview Study of Software Signing for Supply Chain Security 81
Kelechi G. Kalu, Tanmay Singla, Chinenye Okafor, Santiago Torres-Arias, and James C. Davis, *Purdue University*

Voluntary Investment, Mandatory Minimums, or Cyber Insurance: What Minimizes Losses? 101
Adam Hastings and Simha Sethumadhavan, *Columbia University*

A First Look at Governments' Enterprise Security Guidance 119
Kimberly Ruth and Raymond Buernor Obu, *Stanford University;* Ifeoluwa Shode, *Fisk University;* Gavin Li, *Stanford University;* Carrie Gates, *FS-ISAC;* Grant Ho, *University of Chicago;* Zakir Durumeric, *Stanford University*

SoK: Can Synthetic Images Replace Real Data? A Survey of Utility and Privacy of Synthetic Image Generation . . . 139
Yunsung Chung, Yunbei Zhang, Nassir Marrouche, and Jihun Hamm, *Tulane University*

Characterizing and Detecting Propaganda-Spreading Accounts on Telegram 161
Klim Kireev, *EPFL, MPI-SP Max Plank Institute for Security and Privacy;* Yevhen Mykhno, *unaffiliated;* Carmela Troncoso, *EPFL, MPI-SP Max Plank Institute for Security and Privacy;* Rebekah Overdorf, *Ruhr University Bochum (RUB), Research Center Trustworthy Data Science and Security in University Alliance Ruhr, University of Lausanne*

LLM Security and Attacks

GradEscape: A Gradient-Based Evader Against AI-Generated Text Detectors 181
Wenlong Meng, Shuguo Fan, and Chengkun Wei, *Zhejiang University;* Min Chen, *Vrije Universiteit Amsterdam;* Yuwei Li, *National University of Defense Technology and Anhui Province Key Laboratory of Cyberspace Security Situation Awareness and Evaluation;* Yuanchao Zhang, *Mybank, Ant Group;* Zhikun Zhang and Wenzhi Chen, *Zhejiang University*

Provably Robust Multi-bit Watermarking for AI-generated Text 201
Wenjie Qu, Wengrui Zheng, Tianyang Tao, Dong Yin, Yanze Jiang, and Zhihua Tian, *National University of Singapore;* Wei Zou and Jinyuan Jia, *Pennsylvania State University;* Jiaheng Zhang, *National University of Singapore*

HateBench: Benchmarking Hate Speech Detectors on LLM-Generated Content and Hate Campaigns 221
Xinyue Shen, Yixin Wu, Yiting Qu, and Michael Backes, *CISPA Helmholtz Center for Information Security;* Savvas Zannettou, *Delft University of Technology;* Yang Zhang, *CISPA Helmholtz Center for Information Security*

EmbedX: Embedding-Based Cross-Trigger Backdoor Attack Against Large Language Models 241
Nan Yan and Yuqing Li, *Wuhan University;* Xiong Wang, *Huazhong University of Science and Technology;* Jing Chen and Kun He, *Wuhan University;* Bo Li, *Hong Kong University of Science and Technology*

Mind the Inconspicuous: Revealing the Hidden Weakness in Aligned LLMs' Refusal Boundaries 259
Jiahao Yu, Haozheng Luo, Jerry Yao-Chieh Hu, and Yan Chen, *Northwestern University;* Wenbo Guo, *University of California, Santa Barbara;* Han Liu and Xinyu Xing, *Northwestern University*

Game of Arrows: On the (In-)Security of Weight Obfuscation for On-Device TEE-Shielded LLM Partition Algorithms. 279
Pengli Wang, *MOEKey Lab of HCST (PKU), School of Computer Science, Peking University;* Bingyou Dong, *ByteDance;* Yifeng Cai, *MOEKey Lab of HCST (PKU), School of Computer Science, Peking University;* Zheng Zhang, *ByteDance;* Junlin Liu, *MOEKey Lab of HCST (PKU), School of Computer Science, Peking University;* Huanran Xue, Ye Wu, and Yao Zhang, *ByteDance;* Ziqi Zhang, *University of Illinois Urbana-Champaign*

LLMmap: Fingerprinting for Large Language Models 299
Dario Pasquini, *RSAC Labs;* Evgenios M. Kornaropoulos and Giuseppe Ateniese, *George Mason University*

Refusal Is Not an Option: Unlearning Safety Alignment of Large Language Models 319
Minkyoo Song, Hanna Kim, Jaehan Kim, Seungwon Shin, and Sooel Son, *KAIST*

Activation Approximations Can Incur Safety Vulnerabilities in Aligned LLMs: Comprehensive Analysis and Defense 339
Jiawen Zhang and Kejia Chen, *Zhejiang University;* Lipeng He, *University of Waterloo;* Jian Lou and Dan Li, *Sun Yat-sen University;* Zunlei Feng, Mingli Song, Jian Liu, Kui Ren, and Xiaohu Yang, *Zhejiang University*

Software Security 1: Vulnerability Analysis, Exploit Synthesis, and Methodology

Narrowbeer: A Practical Replay Attack Against the Widevine DRM 359
Florian Roudot and Mohamed Sabt, *Univ Rennes, CNRS, IRISA*

Lancet: A Formalization Framework for Crash and Exploit Pathology. 375
Qinrun Dai, Kirby Linvill, Yueqi Chen, and Gowtham Kaki, *University of Colorado Boulder*

Synthesis of Code-Reuse Attacks from p-code Programs. 395
Mark DenHoed and Tom Melham, *University of Oxford*

Sound and Efficient Generation of Data-Oriented Exploits via Programming Language Synthesis 413
Yuxi Ling, *National Univeristy of Singapore;* Gokul Rajiv, *National University of Singapore;* Kiran Gopinathan, *University of Illinois Urbana-Champaign;* Ilya Sergey, *National University of Singapore*

My ZIP isn't your ZIP: Identifying and Exploiting Semantic Gaps Between ZIP Parsers. 431
Yufan You, *Tsinghua University;* Jianjun Chen, *Tsinghua University; Zhongguancun Laboratory;* Qi Wang, *Tsinghua University;* Haixin Duan, *Tsinghua University; Zhongguancun Laboratory*

Tady: A Neural Disassembler without Structural Constraint Violations 451
Siliang Qin, *Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences;* Fengrui Yang and Hao Wang, *Tsinghua University;* Bolun Zhang, *Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences;* Zeyu Gao and Chao Zhang, *Tsinghua University;* Kai Chen, *Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences*

SoK: Towards a Unified Approach to Applied Replicability for Computer Security 469
Daniel Olszewski, Tyler Tucker, Kevin R. B. Butler, and Patrick Traynor, *University of Florida*

LLMxCPG: Context-Aware Vulnerability Detection Through Code Property Graph-Guided Large Language Models. 489
Ahmed Lekssays and Hamza Mouhcine, *Qatar Computing Research Institute;* Khang Tran, *New Jersey Institute of Technology;* Ting Yu, *Mohamed bin Zayed University of Artificial Intelligence;* Issa Khalil, *Qatar Computing Research Institute*

X.509DoS: Exploiting and Detecting Denial-of-Service Vulnerabilities in Cryptographic Libraries using Crafted X.509 Certificates. 509
Bing Shi, Wenchao Li, Yuchen Wang, and Xiaolong Bai, *Alibaba Group;* Luyi Xing, *Indiana University Bloomington*

System Security 1: Threat Detection, Exploitation, and Adaptive Defenses

Cyber-Physical Deception Through Coordinated IoT Honeypots 529
Chongqi Guan and Guohong Cao, *The Pennsylvania State University*

AutoLabel: Automated Fine-Grained Log Labeling for Cyber Attack Dataset Generation 547
Yihao Peng and Tongxin Zhang, *Tsinghua University;* Jieshao Lai, *University of Science and Technology of China;* Yuxuan Zhang, Yiming Wu, Hai Wan, and Xibin Zhao, *Tsinghua University*

CoVault: Secure, Scalable Analytics of Personal Data 567
Roberta De Viti and Isaac Sheff, *Max Planck Institute for Software Systems* (*MPI-SWS*)*, Saarland Informatics Campus;* Noemi Glaeser, *Max Planck Institute for Security and Privacy* (*MPI-SP*) *and University of Maryland;* Baltasar Dinis, *Instituto Superior Técnico* (*ULisboa*)*, INESC-ID;* Rodrigo Rodrigues, *Instituto Superior Técnico* (*ULisboa*) / *INESC-ID;* Bobby Bhattacharjee, *University of Maryland;* Anwar Hithnawi, *ETH Zürich;* Deepak Garg and Peter Druschel, *Max Planck Institute for Software Systems* (*MPI-SWS*)*, Saarland Informatics Campus*

EvilEDR: Repurposing EDR as an Offensive Tool 587
Kotaiba Alachkar, *Delft University of Technology;* Dirk Gaastra, *Independent Researcher;* Eduardo Barbaro, Michel van Eeten, and Yury Zhauniarovich, *Delft University of Technology*

TAPAS: An Efficient Online APT Detection with Task-guided Process Provenance Graph Segmentation and Analysis. 607
Bo Zhang, *Nanjing University of Science and Technology;* Yansong Gao, *The University of Western Australia;* Changlong Yu and Boyu Kuang, *Nanjing University of Science and Technology;* Zhi Zhang, *The University of Western Australia;* Hyoungshick Kim, *Sungkyunkwan University;* Anmin Fu, *Nanjing University of Science and Technology*

Nothing is Unreachable: Automated Synthesis of Robust Code-Reuse Gadget Chains for Arbitrary Exploitation Primitives. 625
Nicolas Bailluet, *Univ Rennes, Inria, CNRS, IRISA;* Emmanuel Fleury, *Univ Bordeaux, CNRS, LaBRI;* Isabelle Puaut and Erven Rohou, *Univ Rennes, Inria, CNRS, IRISA*

BlueGuard: Accelerated Host and Guest Introspection Using DPUs 645
Meni Orenbach, Rami Ailabouni, and Nael Masalha, *NVIDIA;* Thanh Nguyen, *unaffiliated;* Ahmad Saleh, Frank Block, Fritz Alder, Ofir Arkin, and Ahmad Atamli, *NVIDIA*

RollingEvidence: Autoregressive Video Evidence via Rolling Shutter Effect 665
Feng Qian, Lingfeng Zhang, Tao Luo, Shiqi Xu, Zhijun Yu, and Wei Wang, *Ant Group*

From Constraints to Cracks: Constraint Semantic Inconsistencies as Vulnerability Beacons for Embedded Systems 685
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, *University of New South Wales;* Yanyan Zou, Yang Xiao, Naijia Jiang, Yeting Li, Nanyu Zhong, Bingwei Peng, Kunpeng Jian, and 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*

Network Security 1: Censorship, Evasion, and Trustworthy Infrastructure

IRBlock: A Large-Scale Measurement Study of the Great Firewall of Iran 705
Jonas Tai and Karthik Nishanth Sengottuvelavan, *University of British Columbia;* Peter Whiting, *University of Waterloo;* Nguyen Phong Hoang, *University of British Columbia*

Email Spoofing with SMTP Smuggling: How the Shared Email Infrastructures Magnify this Vulnerability 723
Chuhan Wang, *Southeast University and Tsinghua University;* Chenkai Wang, *University of Illinois Urbana-Champaign;* Songyi Yang, *Tsinghua University;* Sophia Liu, *University of Illinois Urbana-Champaign;* Jianjun Chen, *Tsinghua University and Zhongguancun Laboratory;* Haixin Duan, *Tsinghua University and Quan Cheng Laboratory;* Gang Wang, *University of Illinois Urbana-Champaign*

The Silent Danger in HTTP: Identifying HTTP Desync Vulnerabilities with Gray-box Testing. 743
Keran Mu, *Tsinghua University;* Jianjun Chen, Jianwei Zhuge, Qi Li, and Haixin Duan, *Tsinghua University; Zhongguancun Laboratory;* Nick Feamster, *University of Chicago*

Censorship Evasion with Unidentified Protocol Generation **763**
Ryan Wails, *U.S. Naval Research Laboratory and Georgetown University;* Rob Jansen and Aaron Johnson, *U.S. Naval Research Laboratory;* Micah Sherr, *Georgetown University*

Exposing and Circumventing SNI-based QUIC Censorship of the Great Firewall of China **783**
Ali Zohaib, *University of Massachusetts Amherst;* Qiang Zao, *GFW Report;* Jackson Sippe and Abdulrahman Alaraj, *University of Colorado Boulder;* Amir Houmansadr, *University of Massachusetts Amherst;* Zakir Durumeric, *Stanford University;* Eric Wustrow, *University of Colorado Boulder*

***Ares*: Comprehensive Path Hijacking Detection via Routing Tree** **803**
Yinxiang Tao, *Institute of Network Sciences and Cyberspace, Tsinghua University, Beijing, China;* Chengwan Zhang, *unaffiliated;* Changqing An, *Institute of Network Sciences and Cyberspace, Tsinghua University, Beijing, China;* Shuying Zhuang, *Zhongguancun Laboratory, Beijing, China;* Jilong Wang, *Quan Cheng Laboratory, 250103, Jinan, Shandong, China and Institute of Network Sciences and Cyberspace, Tsinghua University, Beijing, China;* Congcong Miao, *Tencent*

Trust but Verify: An Assessment of Vulnerability Tagging Services **823**
Szu-Chun Huang, Harm Griffioen, Max van der Horst, Georgios Smaragdakis, Michel van Eeten, and Yury Zhauniarovich, *Delft University of Technology*

Watch Out Your TV Box: Reversing and Blocking a P2P-based Illegal Streaming Ecosystem **843**
Jungun Ahn, Sueun Jung, Seungwan Yoo, Jungheum Park, and Sangjin Lee, *Korea University*

Catch-22: Uncovering Compromised Hosts using SSH Public Keys **861**
Cristian Munteanu, *Max Planck Institute for Informatics;* Georgios Smaragdakis, *Delft University of Technology;* Anja Feldmann and Tobias Fiebig, *Max Planck Institute for Informatics*

ML and AI Security 1: Images

USD: NSFW Content Detection for Text-to-Image Models via Scene Graph **879**
Yuyang Zhang, *Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University;* Kangjie Chen, *Nanyang Technological University;* Xudong Jiang, Jiahui Wen, Yihui Jin, and Ziyou Liang, *Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University;* Yihao Huang, *National University of Singapore;* Run Wang and Lina Wang, *Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University*

Exposing the Guardrails: Reverse-Engineering and Jailbreaking Safety Filters in DALL·E Text-to-Image Pipelines **897**
Corban Villa, *New York University Abu Dhabi;* Shujaat Mirza, *New York University;* Christina Pöpper, *New York University Abu Dhabi*

On the Proactive Generation of Unsafe Images From Text-To-Image Models Using Benign Prompts **917**
Yixin Wu, *CISPA Helmholtz Center for Information Security;* Ning Yu, *Netflix Eyeline Studios;* Michael Backes, *CISPA Helmholtz Center for Information Security;* Yun Shen, *Netapp;* Yang Zhang, *CISPA Helmholtz Center for Information Security*

Neural Invisibility Cloak: Concealing Adversary in Images via Compromised AI-driven Image Signal Processing . . . **937**
Wenjun Zhu, Xiaoyu Ji, Xinfeng Li, Qihang Chen, Kun Wang, Xinyu Li, Ruoyan Xu, and Wenyuan Xu, *Zhejiang University*

Bridging the Gap in Vision Language Models in Identifying Unsafe Concepts Across Modalities **957**
Yiting Qu, Michael Backes, and Yang Zhang, *CISPA Helmholtz Center for Information Security*

Backdooring Bias (B^2) into Stable Diffusion Models **977**
Ali Naseh, Jaechul Roh, Eugene Bagdasarian, and Amir Houmansadr, *University of Massachusetts Amherst*

Watch the Watchers! On the Security Risks of Robustness-Enhancing Diffusion Models **997**
Changjiang Li, *Stony Brook University;* Ren Pang, Bochuan Cao, Jinghui Chen, and Fenglong Ma, *The Pennsylvania State University;* Shouling Ji, *Zhejiang University;* Ting Wang, *Stony Brook University*

Pretender: Universal Active Defense against Diffusion Finetuning Attacks **1017**
Zekun Sun and Zijian Liu, *Shanghai Jiao Tong University;* Shouling Ji, *Zhejiang University;* Chenhao Lin, *Xi'an Jiaotong University;* Na Ruan, *Shanghai Jiao Tong University*

Self-interpreting Adversarial Images 1037
Tingwei Zhang, Collin Zhang, and John X. Morris, *Cornell Tech;* Eugene Bagdasarian, *University of Massachusetts Amherst;* Vitaly Shmatikov, *Cornell Tech*

System Security 2: Trusted and Robust Computing

TORchlight: Shedding Light on Real-World Attacks on Cloudless IoT Devices Concealed within the Tor Network. 1053
Yumingzhi Pan and Zhen Ling, *Southeast University;* Yue Zhang, *Drexel University;* Hongze Wang, Guangchi Liu, and Junzhou Luo, *Southeast University;* Xinwen Fu, *University of Massachusetts Lowell*

CloudFlow: Identifying Security-sensitive Data Flows in Serverless Applications 1073
Giuseppe Raffa, *Royal Holloway, University of London;* Jorge Blasco, *Universidad Politécnica de Madrid;* Dan O'Keeffe, *Royal Holloway, University of London;* Santanu Kumar Dash, *University of Surrey*

Serverless Functions Made Confidential and Efficient with Split Containers 1091
Jiacheng Shi, Jinyu Gu, Yubin Xia, and Haibo Chen, *Shanghai Jiao Tong University*

Exploring and Exploiting the Resource Isolation Attack Surface of WebAssembly Containers 1111
Zhaofeng Yu, Dongyang Zhan, Lin Ye, Haining Yu, and Hongli Zhang, *Harbin Institute of Technology;* Zhihong Tian, *Guangzhou University*

Transparent Attested DNS for Confidential Computing Services. 1129
Antoine Delignat-Lavaud, Cédric Fournet, Kapil Vaswani, Manuel Costa, and Sylvan Clebsch, *Azure Research, Microsoft;* Christoph M. Wintersteiger, *Imandra*

Dorami: Privilege Separating Security Monitor on RISC-V TEEs 1149
Mark Kuhne, *ETH Zurich;* Stavros Volos, *Azure Research, Microsoft;* Shweta Shinde, *ETH Zurich*

TLBlur: Compiler-Assisted Automated Hardening against Controlled Channels on Off-the-Shelf Intel SGX Platforms. 1167
Daan Vanoverloop, *DistriNet, KU Leuven;* Andrés Sánchez, *EPFL, Amazon;* Flavio Toffalini, *EPFL, RUB;* Frank Piessens, *DistriNet, KU Leuven;* Mathias Payer, *EPFL;* Jo Van Bulck, *DistriNet, KU Leuven*

TETD: Trusted Execution in Trust Domains 1187
Zhanbo Wang, *Research Institute of Trustworthy Autonomous Systems, Southern University of Science and Technology, China, and Pengcheng Laboratory, China;* Jiaxin Zhan, *Research Institute of Trustworthy Autonomous Systems, Southern University of Science and Technology, China, and Department of Computer Science and Engineering, Southern University of Science and Technology, China;* Xuhua Ding, *Singapore Management University;* Fengwei Zhang, *Department of Computer Science and Engineering, Southern University of Science and Technology, China, and Research Institute of Trustworthy Autonomous Systems, Southern University of Science and Technology, China;* Ning Hu, *Pengcheng Laboratory, China*

TDXploit: Novel Techniques for Single-Stepping and Cache Attacks on Intel TDX 1207
Fabian Rauscher, *Graz University of Technology;* Luca Wilke, *University of Lübeck;* Hannes Weissteiner, *Graz University of Technology;* Thomas Eisenbarth, *University of Lübeck;* Daniel Gruss, *Graz University of Technology*

Blockchain Security, Attacks, and Defenses

Auspex: Unveiling Inconsistency Bugs of Transaction Fee Mechanism in Blockchain 1223
Zheyuan He, *University of Electronic Science and Technology of China;* Zihao Li, *The Hong Kong Polytechnic University;* Jiahao Luo, *University of Electronic Science and Technology of China;* Feng Luo, *The Hong Kong Polytechnic University;* Junhan Duan, *Carnegie Mellon University;* Jingwei Li and Shuwei Song, *University of Electronic Science and Technology of China;* Xiapu Luo, *The Hong Kong Polytechnic University;* Ting Chen and Xiaosong Zhang, *University of Electronic Science and Technology of China*

Blockchain Address Poisoning. 1243
Taro Tsuchiya and Jin-Dong Dong, *Carnegie Mellon University;* Kyle Soska, *Independent;* Nicolas Christin, *Carnegie Mellon University*

Available Attestation: Towards a Reorg-Resilient Solution for Ethereum Proof-of-Stake 1263
Mingfei Zhang, *Shandong University;* Rujia Li, *Tsinghua University;* Xueqian Lu, *Independent Reseacher;* Sisi Duan, *Tsinghua University*

Approve Once, Regret Forever: On the Exploitation of Ethereum's Approve-TransferFrom Ecosystem 1281
Nicola Ruaro, Fabio Gritti, Dongyu Meng, and Robert McLaughlin, *University of California, Santa Barbara;* Ilya Grishchenko, *University of Toronto;* Christopher Kruegel and Giovanni Vigna, *University of California, Santa Barbara*

Voting-Bloc Entropy: A New Metric for DAO Decentralization 1299
Andres Fabrega, *Cornell University;* Amy Zhao, *IC3;* Jay Yu, *Stanford University;* James Austgen, *Cornell Tech;* Sarah Allen, *IC3 and Flashbots;* Kushal Babel, *Cornell Tech and IC3;* Mahimna Kelkar, *Cornell Tech;* Ari Juels, *Cornell Tech and IC3*

Deanonymizing Ethereum Validators: The P2P Network Has a Privacy Issue 1319
Lioba Heimbach and Yann Vonlanthen, *ETH Zurich;* Juan Villacis, *University of Bern;* Lucianna Kiffer, *IMDEA Networks;* Roger Wattenhofer, *ETH Zurich*

Let's Move2EVM 1339
Lorenzo Benetollo, *Ca' Foscari University of Venice, University of Camerino, and Christian Doppler Laboratory Blockchain Technologies for the Internet of Things;* Andreas Lackner, *TU Wien;* Matteo Maffei and Markus Scherer, *TU Wien and Christian Doppler Laboratory Blockchain Technologies for the Internet of Things*

Ghost Clusters: Evaluating Attribution of Illicit Services through Cryptocurrency Tracing 1357
Kelvin Lubbertsen, Michel van Eeten, and Rolf van Wegberg, *Delft University of Technology*

Surviving in Dark Forest: Towards Evading the Attacks from Front-Running Bots in Application Layer 1375
Zuchao Ma, Muhui Jiang, Feng Luo, and Xiapu Luo, *The Hong Kong Polytechnic University;* Yajin Zhou, *Zhejiang University*

Usable Privacy and Security 1

SoK: Inaccessible & Insecure: An Exposition of Authentication Challenges Faced by Blind and Visually Impaired Users in State-of-the-Art Academic Proposals 1393
Md Mojibur Rahman Redoy Akanda, Amanda Lacy, and Nitesh Saxena, *Texas A&M University*

Scanned and Scammed: Insecurity by ObsQRity? Measuring User Susceptibility and Awareness of QR Code-Based Attacks 1415
Marvin Kowalewski and Leona Lassak, *Ruhr University Bochum;* Markus Dürmuth, *Leibniz University Hannover;* Theodor Schnitzler, *Maastricht University*

URL Inspection Tasks: Helping Users Detect Phishing Links in Emails 1435
Daniele Lain, Yoshimichi Nakatsuka, and Kari Kostiainen, *ETH Zurich;* Gene Tsudik, *University of California, Irvine;* Srdjan Capkun, *ETH Zurich*

Digital Security Perceptions and Practices Around the World: A WEIRD versus Non-WEIRD Comparison 1455
Franziska Herbert, *Ruhr University Bochum;* Collins W. Munyendo, *The George Washington University and Max Planck Institute for Security and Privacy;* Jonas Hielscher, *Ruhr University Bochum;* Steffen Becker, *Ruhr University Bochum and Max Planck Institute for Security and Privacy;* Yixin Zou, *Max Planck Institute for Security and Privacy*

SoK: Come Together – Unifying Security, Information Theory, and Cognition for a Mixed Reality Deception Attack Ontology & Analysis Framework 1475
Ali Teymourian and Andrew M. Webb, *Division of Computer Science & Engineering, Louisiana State University;* Taha Gharaibeh, *Division of Computer Science & Engineering, Baggil(i) Truth (BiT) Lab, Center for Computation and Technology, Louisiana State University;* Arushi Ghildiyal, *Division of Computer Science & Engineering, Louisiana State University;* Ibrahim Baggili, *Division of Computer Science & Engineering, Baggil(i) Truth (BiT) Lab, Center for Computation and Technology, Louisiana State University*

Am I Infected? Lessons from Operating a Large-Scale IoT Security Diagnostic Service 1493
Takayuki Sasaki, Tomoya Inazawa, and Youhei Yamaguchi, *Yokohama National University;* Simon Parkin and Michel van Eeten, *Delft University of Technology/Yokohama National University;* Katsunari Yoshioka and Tsutomu Matsumoto, *Yokohama National University*

AirTag-Facilitated Stalking Protection: Evaluating Unwanted Tracking Notifications and Tracker Locating Features 1511
Dañiel Gerhardt, *CISPA Helmholtz Center for Information Security and Saarland University;* Matthias Fassl, *CISPA Helmholtz Center for Information Security;* Carolyn Guthoff, *CISPA Helmholtz Center for Information Security and Saarland University;* Adrian Dabrowski, *Research Center IT-Security, University of Applied Sciences FH Campus Wien;* Katharina Krombholz, *CISPA Helmholtz Center for Information Security*

PrivaCI in VR: Exploring Perceptions and Acceptability of Data Sharing in Virtual Reality Through Contextual Integrity 1531
Emiram Kablo and Melina Kleber, *Paderborn University;* Patricia Arias Cabarcos, *Paderborn University and KASTEL Security Research Labs*

Shadowed Realities: An Investigation of UI Attacks in WebXR 1549
Chandrika Mukherjee, *Purdue University;* Reham Mohamed, *American University of Sharjah;* Arjun Arunasalam, *Purdue University;* Habiba Farrukh, *University of California, Irvine;* Z. Berkay Celik, *Purdue University*

LLM Privacy

Unlocking the Power of Differentially Private Zeroth-order Optimization for Fine-tuning LLMs. 1569
Ergute Bao, *Alibaba Group;* Yangfan Jiang, *National University of Singapore;* Fei Wei, *Alibaba Group;* Xiaokui Xiao, *National University of Singapore;* Zitao Li, Yaliang Li, and Bolin Ding, *Alibaba Group*

Membership Inference Attacks Against Vision-Language Models 1589
Yuke Hu, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University;* Zheng Li, *Shandong University;* Zhihao Liu, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University;* Yang Zhang, *CISPA Helmholtz Center for Information Security;* Zhan Qin, Kui Ren, and Chun Chen, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University*

Towards Label-Only Membership Inference Attack against Pre-trained Large Language Models 1609
Yu He, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University;* Boheng Li, *College of Computing and Data Science, Nanyang Technological University;* Liu Liu and Zhongjie Ba, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University;* Wei Dong, *College of Computing and Data Science, Nanyang Technological University;* Yiming Li, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University; and College of Computing and Data Science, Nanyang Technological University;* Zhan Qin, Kui Ren, and Chun Chen, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University*

Depth Gives a False Sense of Privacy: LLM Internal States Inversion. 1629
Tian Dong and Yan Meng, *Shanghai Jiao Tong University;* Shaofeng Li, *Southeast University;* Guoxing Chen, Zhen Liu, and Haojin Zhu, *Shanghai Jiao Tong University*

I Know What You Said: Unveiling Hardware Cache Side-Channels in Local Large Language Model Inference . . . 1649
Zibo Gao, Junjie Hu, Feng Guo, Yixin Zhang, Yinglong Han, Siyuan Liu, Haiyang Li, and Zhiqiang Lv, *Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences*

Evaluating LLM-based Personal Information Extraction and Countermeasures. 1669
Yupei Liu, *The Pennsylvania State University;* Yuqi Jia, *Duke University;* Jinyuan Jia, *The Pennsylvania State University;* Neil Zhenqiang Gong, *Duke University*

Synthetic Artifact Auditing: Tracing LLM-Generated Synthetic Data Usage in Downstream Applications 1689
Yixin Wu and Ziqing Yang, *CISPA Helmholtz Center for Information Security;* Yun Shen, *Netapp;* Michael Backes and Yang Zhang, *CISPA Helmholtz Center for Information Security*

Data-Free Model-Related Attacks: Unleashing the Potential of Generative AI 1709
Dayong Ye, *University of Technology Sydney;* Tianqing Zhu, *City University of Macau;* Shang Wang and Bo Liu, *University of Technology Sydney;* Leo Yu Zhang, *Griffith University;* Wanlei Zhou, *City University of Macau;* Yang Zhang, *CISPA Helmholtz Center for Information Security*

When LLMs Go Online: The Emerging Threat of Web-Enabled LLMs 1729
Hanna Kim, Minkyoo Song, Seung Ho Na, Seungwon Shin, and Kimin Lee, *Korea Advanced Institute of Science and Technology* (*KAIST*)

Embedded and Hardware Security

Enabling Low-Cost Secure Computing on Untrusted In-Memory Architectures 1749
Sahar Ghoflsaz Ghinani, Jingyao Zhang, and Elaheh Sadredini, *University of California, Riverside*

AidFuzzer: Adaptive Interrupt-Driven Firmware Fuzzing via Run-Time State Recognition 1769
Jianqiang Wang, *CISPA Helmholtz Center for Information Security;* Qinying Wang, *Zhejiang University;* Tobias Scharnowski, *CISPA Helmholtz Center for Information Security;* Li Shi, *ETH Zurich;* Simon Woerner and Thorsten Holz, *CISPA Helmholtz Center for Information Security*

GenHuzz: An Efficient Generative Hardware Fuzzer 1787
Lichao Wu, Mohamadreza Rostami, and Huimin Li, *Technical University of Darmstadt;* Jeyavijayan Rajendran, *Texas A&M University;* Ahmad-Reza Sadeghi, *Technical University of Darmstadt*

Software Availability Protection in Cyber-Physical Systems 1807
Ao Li, Jinwen Wang, and Ning Zhang, *Washington University in St. Louis*

GDMA: Fully Automated DMA Rehosting via Iterative Type Overlays. 1827
Tobias Scharnowski, Simeon Hoffmann, Moritz Bley, and Simon Wörner, *CISPA Helmholtz Center for Information Security;* Daniel Klischies, *Ruhr-Universität Bochum;* Felix Buchmann, Nils Ole Tippenhauer, and Thorsten Holz, *CISPA Helmholtz Center for Information Security;* Marius Muench, *University of Birmingham*

KINTSUGI: Secure Hotpatching for Code-Shadowing Real-Time Embedded Systems 1847
Philipp Mackensen, *Ruhr University Bochum;* Christian Niesler, *University of Duisburg-Essen;* Roberto Blanco, *Eindhoven University of Technology/MPI-SP;* Lucas Davi, *University of Duisburg-Essen;* Veelasha Moonsamy, *Ruhr University Bochum*

Security Implications of Malicious G-Codes in 3D Printing 1867
Jost Rossel, *Paderborn University;* Vladislav Mladenov, *Ruhr University Bochum;* Nico Wördenweber and Juraj Somorovsky, *Paderborn University*

Secure Information Embedding in Forensic 3D Fingerprinting 1887
Canran Wang, Jinwen Wang, Mi Zhou, Vinh Pham, Senyue Hao, Chao Zhou, Ning Zhang, and Netanel Raviv, *Washington University in St. Louis*

SoK: A Security Architect's View of Printed Circuit Board Attacks 1907
Jacob Harrison, *Bloomberg L.P.;* Nathan Jessurun, *Terraverum;* Mark Tehranipoor, *University of Florida*

Crypto 1: Zero Knowledge and Multi-Party Computation

Dumbo-MPC: Efficient Fully Asynchronous MPC with Optimal Resilience 1925
Yuan Su, *Xi'an Jiaotong University;* Yuan Lu, *Institute of Software Chinese Academy of Sciences;* Jiliang Li, *Xi'an Jiaotong University;* Yuyi Wang, *CRRC Zhuzhou Institute;* Chengyi Dong, *Xi'an Jiaotong University;* Qiang Tang, *The University of Sydney*

FABLE: Batched Evaluation on Confidential Lookup Tables in 2PC. 1945
Zhengyuan Su, *Tsinghua University;* Qi Pang, Simon Beyzerov, and Wenting Zheng, *Carnegie Mellon University*

MAESTRO: Multi-Party AES Using Lookup Tables. 1965
Hiraku Morita, *Aarhus University and University of Copenhagen;* Erik Pohle, *COSIC, KU Leuven;* Kunihiko Sadakane, *The University of Tokyo;* Peter Scholl, *Aarhus University;* Kazunari Tozawa, *The University of Tokyo;* Daniel Tschudi, *Concordium and Eastern Switzerland University of Applied Sciences* (*OST*)

Efficient 2PC for Constant Round Secure Equality Testing and Comparison. 1985
Tianpei Lu, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University;* Xin Kang, *Xidian University;* Bingsheng Zhang, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University; and Hangzhou High-Tech Zone* (*Binjiang*) *Institute of Blockchain and Data Security;* Zhuo Ma, *Xidian University;* Xiaoyuan Zhang, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University;* Yang Liu, *Xidian University;* Kui Ren and Chun Chen, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University*

Efficient Multi-Party Private Set Union Without Non-Collusion Assumptions 2005
Minglang Dong, *School of Cyber Science and Technology, Shandong University; Quan Cheng Laboratory; Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University;* Cong Zhang, *Institute for Advanced Study, BNRist, Tsinghua University;* Yujie Bai and Yu Chen, *School of Cyber Science and Technology, Shandong University; Quan Cheng Laboratory; Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University*

Scalable Collaborative zk-SNARK and Its Application to Fully Distributed Proof Delegation 2025
Xuanming Liu, Zhelei Zhou, and Yinghao Wang, *Zhejiang University;* Yanxin Pang, *Tsinghua University;* Jinye He, *University of Virginia;* Bingsheng Zhang and Xiaohu Yang, *Zhejiang University;* Jiaheng Zhang, *National University of Singapore*

zkGPT: An Efficient Non-interactive Zero-knowledge Proof Framework for LLM Inference 2045
Wenjie Qu, *National University of Singapore;* Yijun Sun, *Hong Kong University of Science and Technology;* Xuanming Liu, Tao Lu, and Yanpei Guo, *National University of Singapore;* Kai Chen, *Hong Kong University of Science and Technology;* Jiaheng Zhang, *National University of Singapore*

DFS: Delegation-friendly zkSNARK and Private Delegation of Provers 2065
Yuncong Hu, *Shanghai Jiao Tong University;* Pratyush Mishra, *University of Pennsylvania;* Xiao Wang, *Northwestern University;* Jie Xie, *Shanghai Jiao Tong University;* Kang Yang, *State Key Laboratory of Cryptology;* Yu Yu, *Shanghai Jiao Tong University and Shanghai Qi Zhi Institute;* Yuwen Zhang, *University of California, Berkeley*

SoK: Understanding zk-SNARKs: The Gap Between Research and Practice 2085
Junkai Liang and Daqi Hu, *Peking University;* Pengfei Wu, *Singapore Management University;* Yunbo Yang, *East China Normal University;* Qingni Shen and Zhonghai Wu, *Peking University*

Thursday, August 14

Usable Privacy and Security 2: Software and Experts

A Mixed-Methods Study of Open-Source Software Maintainers On Vulnerability Management and Platform Security Features 2105
Jessy Ayala, Yu-Jye Tung, and Joshua Garcia, *University of California, Irvine*

"Threat modeling is very formal, it's very technical, and also very hard to do correctly": Investigating Threat Modeling Practices in Open-Source Software Projects 2125
Harjot Kaur, *CISPA Helmholtz Center for Information Security;* Carson Powers and Ronald E. Thompson III, *Tufts University;* Sascha Fahl, *CISPA Helmholtz Center for Information Security;* Daniel Votipka, *Tufts University*

"I wasn't sure if this is indeed a security risk": Data-driven Understanding of Security Issue Reporting in GitHub Repositories of Open Source npm Packages 2145
Rajdeep Ghosh, Shiladitya De, and Mainack Mondal, *IIT Kharagpur*

Context Matters: Qualitative Insights into Developers' Approaches and Challenges with Software Composition Analysis 2165
Elizabeth Lin, Sparsha Gowda, William Enck, and Dominik Wermke, *NC State University*

Expert Insights into Advanced Persistent Threats: Analysis, Attribution, and Challenges 2185
Aakanksha Saha, *Technische Universität Wien;* James Mattei, *Tufts University;* Jorge Blasco, *Universidad Politécnica de Madrid;* Lorenzo Cavallaro, *University College London;* Daniel Votipka, *Tufts University;* Martina Lindorfer, *Technische Universität Wien*

How Researchers De-Identify Data in Practice 2205
Wentao Guo, *University of Maryland;* Paige Pepitone, *NORC at the University of Chicago;* Adam J. Aviv, *The George Washington University;* Michelle L. Mazurek, *University of Maryland*

A limited technical background is sufficient for attack-defense tree acceptability 2225
Nathan Daniel Schiele and Olga Gadyatskaya, *Leiden University*

"It's not my responsibility to write them": An Empirical Study of Software Product Managers and Security Requirements 2245
Houda Naji, Felix Reichmann, Tobias Bruns, and M. Angela Sasse, *Ruhr University Bochum;* Alena Naiakshina, *University of Cologne*

Patching Up: Stakeholder Experiences of Security Updates for Connected Medical Devices 2265
Lorenz Kustosch, Carlos Gañán, Michel van Eeten, and Simon Parkin, *TU Delft*

LLM Security 2: Jailbreaking and Prompt Stealing

PRSA: Prompt Stealing Attacks against Real-World Prompt Services 2283
Yong Yang, *Zhejiang University;* Changjiang Li, *Stony Brook University;* Qingming Li, Oubo Ma, Haoyu Wang, Zonghui Wang, Yandong Gao, Wenzhi Chen, and Shouling Ji, *Zhejiang University*

Cross-Modal Prompt Inversion: Unifying Threats to Text and Image Generative AI Models 2303
Dayong Ye and Tianqing Zhu, *City University of Macau;* Feng He and Bo Liu, *University of Technology Sydney;* Minhui Xue, *CSIRO's Data61;* Wanlei Zhou, *City University of Macau*

Prompt Obfuscation for Large Language Models 2323
David Pape and Sina Mavali, *CISPA Helmholtz Center for Information Security;* Thorsten Eisenhofer, *Berlin Institute for the Foundations of Learning and Data* (*BIFOLD*) *and Technische Universität Berlin;* Lea Schönherr, *CISPA Helmholtz Center for Information Security*

TwinBreak: Jailbreaking LLM Security Alignments based on Twin Prompts 2343
Torsten Krauß, Hamid Dashtbani, and Alexandra Dmitrienko, *University of Würzburg*

Exploiting Task-Level Vulnerabilities: An Automatic Jailbreak Attack and Defense Benchmarking for LLMs . . 2363
Lan Zhang and Xinben Gao, *University of Science and Technology of China;* Liuyi Yao; Jinke Song, *The Hong Kong University of Science and Technology;* Yaliang Li

StruQ: Defending Against Prompt Injection with Structured Queries 2383
Sizhe Chen, Julien Piet, Chawin Sitawarin, and David Wagner, *UC Berkeley*

Papillon: Efficient and Stealthy Fuzz Testing-Powered Jailbreaks for LLMs 2401
Xueluan Gong, *Nanyang Technological University;* Mingzhe Li, Yilin Zhang, and Fengyuan Ran, *Wuhan University;* Chen Chen, *Nanyang Technological University;* Yanjiao Chen, *Zhejiang University;* Qian Wang, *Wuhan University;* Kwok-Yan Lam, *Nanyang Technological University*

Great, Now Write an Article About That: The Crescendo Multi-Turn LLM Jailbreak Attack 2421
Mark Russinovich, *Microsoft Azure;* Ahmed Salem and Ronen Eldan, *Microsoft*

SelfDefend: LLMs Can Defend Themselves against Jailbreaking in a Practical Manner 2441
Xunguang Wang, Daoyuan Wu, Zhenlan Ji, Zongjie Li, Pingchuan Ma, and Shuai Wang, *The Hong Kong University of Science and Technology;* Yingjiu Li, *University of Oregon;* Yang Liu, *Nanyang Technological University;* Ning Liu, *City University of Hong Kong;* Juergen Rahmel, *HSBC*

Hardware Security 1: Microarchitectures

SoK: So, You Think You Know All About Secure Randomized Caches? 2461
Anubhav Bhatla, Hari Rohit Bhavsar, Sayandeep Saha, and Biswabandan Panda, *Indian Institute of Technology Bombay*

TEEcorrelate: An Information-Preserving Defense against Performance-Counter Attacks on TEEs 2481
Hannes Weissteiner and Fabian Rauscher, *Graz University of Technology;* Robin Leander Schröder, *Fraunhofer SIT and Fraunhofer Austria;* Jonas Juffinger and Stefan Gast, *Graz University of Technology;* Jan Wichelmann and Thomas Eisenbarth, *University Luebeck;* Daniel Gruss, *Graz University of Technology*

Systematic Evaluation of Randomized Cache Designs against Cache Occupancy 2499
Anirban Chakraborty, *Max Planck Institute for Security and Privacy;* Nimish Mishra, *Indian Institute of Technology Kharagpur;* Sayandeep Saha, *Indian Institute of Technology Bombay;* Sarani Bhattacharya and Debdeep Mukhopadhyay, *Indian Institute of Technology Kharagpur*

Exploiting Inaccurate Branch History in Side-Channel Attacks 2519
Yuhui Zhu, *Scuola Superiore Sant'Anna and Scuola IMT Alti Studi Lucca;* Alessandro Biondi, *Scuola Superiore Sant'Anna*

Phantom Trails: Practical Pre-Silicon Discovery of Transient Data Leaks 2539
Alvise de Faveri Tron, Raphael Isemann, Hany Ragab, Cristiano Giuffrida, Klaus von Gleissenthall, and Herbert Bos, *Vrije Universiteit Amsterdam*

Place Protections at the Right Place: Targeted Hardening for Cryptographic Code against Spectre v1 2557
Yiming Zhu, Wenchao Huang, and Yan Xiong, *University of Science and Technology of China*

Encarsia: Evaluating CPU Fuzzers via Automatic Bug Injection 2577
Matej Bölcskei, Flavien Solt, Katharina Ceesay-Seitz, and Kaveh Razavi, *ETH Zurich*

FLOP: Breaking the Apple M3 CPU via False Load Output Predictions 2595
Jason Kim, Jalen Chuang, and Daniel Genkin, *Georgia Tech;* Yuval Yarom, *Ruhr University Bochum*

Branch Privilege Injection: Compromising Spectre v2 Hardware Mitigations by Exploiting Branch Predictor Race Conditions 2615
Sandro Rüegge, Johannes Wikner, and Kaveh Razavi, *ETH Zurich*

Privacy 1: Differential Privacy and Audit

GraphAce: Secure Two-Party Graph Analysis Achieving Communication Efficiency 2633
Jiping Yu, *Tsinghua University and Ant Group;* Kun Chen, *Ant Group;* Yunyi Chen and Xiaoyu Fan, *Tsinghua University and Ant Group;* Xiaowei Zhu and Cheng Hong, *Ant Group;* Wenguang Chen, *Tsinghua University and Ant Group*

Breaking the Layer Barrier: Remodeling Private Transformer Inference with Hybrid CKKS and MPC 2653
Tianshi Xu, *Peking University;* Wen-jie Lu, *TikTok;* Jiangrui Yu, Yi Chen, Chenqi Lin, Runsheng Wang, and Meng Li, *Peking University*

HawkEye: Statically and Accurately Profiling the Communication Cost of Models in Multi-party Learning 2673
Wenqiang Ruan, Xin Lin, Ruisheng Zhou, and Guopeng Lin, *Fudan University;* Shui Yu, *University of Technology Sydney;* Weili Han, *Fudan University*

Privacy Audit as Bits Transmission: (Im)possibilities for Audit by One Run 2693
Zihang Xiang, *KAUST;* Tianhao Wang, *University of Virginia;* Di Wang, *KAUST*

General-Purpose *f*-DP Estimation and Auditing in a Black-Box Setting 2713
Önder Askin, Holger Dette, and Martin Dunsche, *Ruhr-University Bochum;* Tim Kutta, *Aarhus University;* Yun Lu, *University of Victoria;* Yu Wei and Vassilis Zikas, *Georgia Institute of Technology*

FastLloyd: Federated, Accurate, Secure, and Tunable *k*-Means Clustering with Differential Privacy 2733
Abdulrahman Diaa, Thomas Humphries, and Florian Kerschbaum, *University of Waterloo*

Addressing Sensitivity Distinction in Local Differential Privacy: A General Utility-Optimized Framework 2753
Xingyu He, Youwen Zhu, and Rongke Liu, *Nanjing University of Aeronautics and Astronautics;* Gaoning Pan, *Hangzhou Dianzi University;* Changyu Dong, *Guangzhou University*

Further Study on Frequency Estimation under Local Differential Privacy 2771
Huiyu Fang, Liquan Chen, and Suhui Liu, *Southeast University*

Beyond Statistical Estimation: Differentially Private Individual Computation via Shuffling 2789
Shaowei Wang and Changyu Dong, *Guangzhou University;* Xiangfu Song, *National University of Singapore;* Jin Li, *Guangzhou University and Guangdong Key Laboratory of Blockchain Security* (*Guangzhou University*)*;* Zhili Zhou, *Guangzhou University;* Di Wang, *King Abdullah University of Science and Technology* (*KAUST*)*;* Han Wu, *University of Southampton*

Software Security and Usable Security

Stack Overflow Meets Replication: Security Research Amid Evolving Code Snippets 2809
Alfusainey Jallow, *CISPA Helmholtz Center for Information Security and Saarland University;* Sven Bugiel, *CISPA Helmholtz Center for Information Security*

"I'm regretting that I hit run": In-situ Assessment of Potential Malware 2829
Brandon Lit, Edward Crowder, and Hassan Khan, *University of Guelph;* Daniel Vogel, *University of Waterloo*

Beyond Exploit Scanning: A Functional Change-Driven Approach to Remote Software Version Identification . . 2847
Jinsong Chen, Mengying Wu, Geng Hong, and Baichao An, *Fudan University;* Mingxuan Liu, *Zhongguancun Laboratory;* Lei Zhang, *Fudan University;* Baojun Liu, *Tsinghua University;* Haixin Duan, *Tsinghua University and Quancheng Laboratory;* Min Yang, *Fudan University*

"I'm trying to learn. . . and I'm shooting myself in the foot": Beginners' Struggles When Solving Binary Exploitation Exercises 2867
James Mattei, Christopher Pellegrini, and Matthew Soto, *Tufts University;* Marina Sanusi Bohuk, *MetaCTF;* Daniel Votipka, *Tufts University*

***Confusing Value with Enumeration*: Studying the Use of CVEs in Academia 2887**
Moritz Schloegel, *CISPA Helmholtz Center for Information Security;* Daniel Klischies, *Ruhr University Bochum;* Simon Koch and David Klein, *TU Braunschweig;* Lukas Gerlach, *CISPA Helmholtz Center for Information Security;* Malte Wessels, *TU Braunschweig;* Leon Trampert, *CISPA Helmholtz Center for Information Security;* Martin Johns, *TU Braunschweig;* Mathy Vanhoef, *DistriNet, KU Leuven;* Michael Schwarz and Thorsten Holz, *CISPA Helmholtz Center for Information Security;* Jo Van Bulck, *DistriNet, KU Leuven*

"That's my perspective from 30 years of doing this": An Interview Study on Practices, Experiences, and Challenges of Updating Cryptographic Code 2907
Alexander Krause, Harjot Kaur, Jan H. Klemmer, Oliver Wiese, and Sascha Fahl, *CISPA Helmholtz Center for Information Security*

***"I have no idea how to make it safer"*: Studying Security and Privacy Mindsets of Browser Extension Developers . . 2927**
Shubham Agarwal and Rafael Mrowczynski, *CISPA Helmholtz Center for Information Security;* Maria Hellenthal, *CISPA Helmholtz Centre for Information Security;* Ben Stock, *CISPA Helmholtz Center for Information Security*

Precise and Effective Gadget Chain Mining through Deserialization Guided Call Graph Construction. 2947
Yiheng Zhang, Ming Wen, and Shunjie Liu, *Huazhong University of Science and Technology;* Dongjie He, *Chongqing University;* Hai Jin, *Huazhong University of Science and Technology*

Mitigating Injection Attacks against E2EE Applications via View-Based Partitioning 2965
Andrés Fábrega, Samuel Breckenridge, and Armin Namavari, *Cornell University;* Thomas Ristenpart, *Cornell Tech*

ML and AI Privacy 1: Federated Learning and Protecting Data

Boosting Gradient Leakage Attacks: Data Reconstruction in Realistic FL Settings. 2985
Mingyuan Fan, *East China Normal University;* Fuyi Wang, *RMIT University;* Cen Chen, *East China Normal University;* Jianying Zhou, *Singapore University of Technology and Design*

***Refiner*: Data Refining against Gradient Leakage Attacks in Federated Learning 3005**
Mingyuan Fan, *East China Normal University;* Cen Chen, *East China Normal University and The State Key Laboratory of Blockchain and Data Security, Zhejiang University;* Chengyu Wang, *Alibaba Group;* Xiaodan Li, *East China Normal University and Alibaba Group;* Wenmeng Zhou, *Alibaba Group*

Aion: Robust and Efficient Multi-Round Single-Mask Secure Aggregation Against Malicious Participants 3025
Yizhong Liu, Zixiao Jia, Zian Jin, Xiao Chen, Song Bian, Runhua Xu, Dawei Li, and Jianwei Liu, *Beihang University;* Yuan Lu, *Institute of Software, Chinese Academy of Sciences*

SoK: On Gradient Leakage in Federated Learning 3045
Jiacheng Du and Jiahui Hu, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University, P. R. China; Hangzhou High-Tech Zone* (*Binjiang*) *Institute of Blockchain and Data Security, P. R. China; and College of Computer Science and Electronic Engineering, Hunan University, P. R. China;* Zhibo Wang, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University, P. R. China; Hangzhou High-Tech Zone* (*Binjiang*) *Institute of Blockchain and Data Security, P. R. China;* Peng Sun, *College of Computer Science and Electronic Engineering, Hunan University, P. R. China;* Neil Gong, *Department of Electrical and Computer Engineering, Duke University, USA;* Kui Ren and Chun Chen, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University, P. R. China; Hangzhou High-Tech Zone* (*Binjiang*) *Institute of Blockchain and Data Security, P. R. China*

DP-BREM: Differentially-Private and Byzantine-Robust Federated Learning with Client Momentum 3065
Xiaolan Gu and Ming Li, *University of Arizona;* Li Xiong, *Emory University*

SLOTHE : Lazy Approximation of Non-Arithmetic Neural Network Functions over Encrypted Data 3083
Kevin Nam, Youyeon Joo, Seungjin Ha, and Yunheung Paek, *Seoul National University*

Sharpness-Aware Initialization: Improving Differentially Private Machine Learning from First Principles 3103
Zihao Wang, Rui Zhu, and Dongruo Zhou, *Indiana University Bloomington;* Zhikun Zhang, *Zhejiang University;* XiaoFeng Wang, *Nanyang Technological University;* Haixu Tang, *Indiana University Bloomington*

Task-Oriented Training Data Privacy Protection for Cloud-based Model Training 3123
Zhiqiang Wang, Jiahui Hou, Haifeng Sun, Jingmiao Zhang, Yunhao Yao, Haikuo Yu, and Xiang-Yang Li, *University of Science and Technology of China*

From Risk to Resilience: Towards Assessing and Mitigating the Risk of Data Reconstruction Attacks in Federated Learning 3141
Xiangrui Xu, *Beijing Jiaotong University;* Zhize Li, *Singapore Management University;* Yufei Han, *INRIA Rennes-Bretagne-Atlantique;* Bin Wang, *Zhejiang Key Laboratory of AIoT Network and Data Security;* Jiqiang Liu, *Beijing Jiaotong University;* Wei Wang, *Beijing Jiaotong University & Xi'an Jiaotong University*

Web and Mobile Security

Demystifying the (In)Security of QR Code-based Login in Real-world Deployments. 3161
Xin Zhang, Xiaohan Zhang, and Bo Zhao, *Fudan University;* Yuhong Nan, *Sun Yat-sen University;* Zhichen Liu, Jianzhou Chen, Huijun Zhou, and Min Yang, *Fudan University*

Doubly Dangerous: Evading Phishing Reporting Systems by Leveraging Email Tracking Techniques. 3181
Anish Chand, *Louisiana State University;* Nick Nikiforakis, *Stony Brook University;* Phani Vadrevu, *Louisiana State University*

Evaluating the Effectiveness and Robustness of Visual Similarity-based Phishing Detection Models 3201
Fujiao Ji and Kiho Lee, *University of Tennessee, Knoxville;* Hyungjoon Koo, *Sungkyunkwan University;* Wenhao You and Euijin Choo, *University of Alberta;* Hyoungshick Kim, *Sungkyunkwan University;* Doowon Kim, *University of Tennessee, Knoxville*

Universal Cross-app Attacks: Exploiting and Securing OAuth 2.0 in Integration Platforms 3221
Kaixuan Luo and Xianbo Wang, *The Chinese University of Hong Kong;* Pui Ho Adonis Fung, *Samsung Research America;* Wing Cheong Lau, *The Chinese University of Hong Kong;* Julien Lecomte, *Samsung Research America*

Predictive Response Optimization: Using Reinforcement Learning to Fight Online Social Network Abuse. 3239
Garrett Wilson, Geoffrey Goh, Yan Jiang, Ajay Gupta, Jiaxuan Wang, David Freeman, and Francesco Dinuzzo, *Meta Platforms, Inc.*

Hercules Droidot and the murder on the JNI Express 3257
Luca Di Bartolomeo and Philipp Mao, *EPFL;* Yu-Jye Tung and Jessy Ayala, *University of California, Irvine;* Samuele Doria, *University of Padua;* Paolo Celada and Marcel Busch, *EPFL;* Joshua Garcia, *University of California, Irvine;* Eleonora Losiouk, *University of Padova;* Mathias Payer, *EPFL*

No Way to Sign Out? Unpacking Non-Compliance with Google Play's App Account Deletion Requirements. 3277
Jingwen Yan, *Clemson University;* Song Liao, *Texas Tech University;* Jin Ma and Mohammed Aldeen, *Clemson University;* Salish Kumar, *Texas Tech University;* Long Cheng, *Clemson University*

Lost in the Mists of Time: Expirations in DNS Footprints of Mobile Apps 3297
Johnny So, *Stony Brook University;* Iskander Sanchez-Rola, *Norton Research Group;* Nick Nikiforakis, *Stony Brook University*

TapTrap: Animation-Driven Tapjacking on Android. 3317
Philipp Beer and Marco Squarcina, *TU Wien;* Sebastian Roth, *University of Bayreuth;* Martina Lindorfer, *TU Wien*

Crypto 2: Private Information Retrieval and Computation

BulletCT: Towards More Scalable Ring Confidential Transactions With Transparent Setup 3337
Nan Wang, *CSIRO's Data61, Australia;* Qianhui Wang, *University of Cambridge;* Dongxi Liu, *CSIRO's Data61, Australia;* Muhammed F. Esgin, *Monash University;* Alsharif Abuadbba, *CSIRO's Data61, Australia*

PolySys: an Algebraic Leakage Attack Engine 3357
Zachary Espiritu, *MongoDB Research;* Seny Kamara, *Brown University and MongoDB Research;* Tarik Moataz, *MongoDB Research;* Andrew Park, *Carnegie Mellon University and MongoDB Research*

Distributional Private Information Retrieval 3377
Ryan Lehmkuhl, Alexandra Henzinger, and Henry Corrigan-Gibbs, *MIT*

Practical Keyword Private Information Retrieval from Key-to-Index Mappings 3397
Meng Hao, *School of Computing & Information Systems, Singapore Management University;* Weiran Liu and Liqiang Peng, *Alibaba Group;* Cong Zhang, *Institute for Advanced Study, BNRist, Tsinghua University;* Pengfei Wu, *School of Computing & Information Systems, Singapore Management University;* Lei Zhang, *Alibaba Group;* Hongwei Li, *Peng Cheng Laboratory;* Robert H. Deng, *School of Computing & Information Systems, Singapore Management University*

SEAF: Secure Evaluation on Activation Functions with Dynamic Precision for Secure Two-Party Inference 3417
Hao Guo and Zhaoqian Liu, *The Chinese University of Hong Kong, Shenzhen;* Ximing Fu, *Harbin Institute of Technology, Shenzhen; Pengcheng Laboratory; Key Laboratory of Cyberspace and Data Security, Ministry of Emergency Management;* Zhusen Liu, *Hangzhou Innovation Institute of Beihang University*

Fast Enhanced Private Set Union in the Balanced and Unbalanced Scenarios 3437
Binbin Tu and Yujie Bai, *School of Cyber Science and Technology, Shandong University; Quan Cheng Laboratory; Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University;* Cong Zhang, *Institute for Advanced Study, BNRist, Tsinghua University;* Yang Cao and Yu Chen, *School of Cyber Science and Technology, Shandong University; Quan Cheng Laboratory; Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University*

BEAT-MEV: Epochless Approach to Batched Threshold Encryption for MEV Prevention 3457
Jan Bormet, Sebastian Faust, Hussien Othman, and Ziyan Qu, *Technische Universität Darmstadt*

Practical Mempool Privacy via One-time Setup Batched Threshold Encryption 3477
Arka Rai Choudhuri, *Nexus;* Sanjam Garg and Guru Vamsi Policharla, *University of California, Berkeley;* Mingyuan Wang, *NYU Shanghai*

DeepFold: Efficient Multilinear Polynomial Commitment from Reed-Solomon Code and Its Application to Zero-knowledge Proofs 3497
Yanpei Guo, Xuanming Liu, Kexi Huang, Wenjie Qu, Tianyang Tao, and Jiaheng Zhang, *National University of Singapore*

Network Security 2: Routing and DoS

Your Shield is My Sword: A Persistent Denial-of-Service Attack via the Reuse of Unvalidated Caches in DNSSEC Validation 3517
Shuhan Zhang, *Tsinghua University and Tsinghua Shenzhen International Graduate School;* Shuai Wang and Li Chen, *Zhongguancun Laboratory;* Dan Li and Baojun Liu, *Tsinghua University*

POPS: From History to Mitigation of DNS Cache Poisoning Attacks 3537
Yehuda Afek, *Tel Aviv University;* Harel Berger, *Ariel University;* Anat Bremler-Barr, *Tel Aviv University*

DNS FLaRE: A Flush-Reload Attack on DNS Forwarders 3557
Gilad Moav, Yehuda Afek, and Anat Bremler-Barr, *Tel Aviv University;* Amit Klein, *Hebrew University of Jerusalem*

Lemon: Network-Wide DDoS Detection with Routing-Oblivious Per-Flow Measurement 3577
Wenhao Wu, Zhenyu Li, and Xilai Liu, *Institute of Computing Technology, Chinese Academy of Sciences; University of Chinese Academy of Sciences;* Zhaohua Wang and Heng Pan, *Computer Network Information Center, Chinese Academy of Sciences;* Guangxing Zhang, *Institute of Computing Technology, Chinese Academy of Sciences;* Gaogang Xie, *Computer Network Information Center, Chinese Academy of Sciences; University of Chinese Academy of Sciences*

Assessing the Aftermath: the Effects of a Global Takedown against DDoS-for-hire Services 3595
Anh V. Vu, *University of Cambridge;* Ben Collier, *University of Edinburgh;* Daniel R. Thomas, *University of Strathclyde;* John Kristoff, *University of Illinois Chicago;* Richard Clayton and Alice Hutchings, *University of Cambridge*

BGP Vortex: Update Message Floods Can Create Internet Instabilities 3613
Felix Stöger, *ETH Zurich;* Henry Birge-Lee, *Princeton University;* Giacomo Giuliari, *Mysten Labs;* Jordi Subira-Nieto and Adrian Perrig, *ETH Zurich*

ImpROV: Measurement and Practical Mitigation of Collateral Damage in RPKI Route Origin Validation 3631
Weitong Li, Yuze Li, and Taejoong Chung, *Virginia Tech*

SoK: An Introspective Analysis of RPKI Security 3649
Donika Mirdita, *Technical University Darmstadt, ATHENE;* Haya Schulmann, *Goethe-University Frankfurt, ATHENE;* Michael Waidner, *Technical University Darmstadt, ATHENE*

Onions Got Puzzled: On the Challenges of Mitigating Denial-of-Service Problems in Tor Onion Services 3667
Jinseo Lee, Hobin Kim, and Min Suk Kang, *KAIST*

LLM Security 3: Hallucinations, RAG Poisoning, and Agentic Attacks

We Have a Package for You! A Comprehensive Analysis of Package Hallucinations by Code Generating LLMs . . . 3687
Joseph Spracklen, Raveen Wijewickrama, and A H M Nazmus Sakib, *University of Texas at San Antonio;* Anindya Maiti, *University of Oklahoma;* Bimal Viswanath, *Virginia Tech;* Murtuza Jadliwala, *University of Texas at San Antonio*

***Mirage in the Eyes*: Hallucination Attack on Multi-modal Large Language Models with *Only* Attention Sink 3707**
Yining Wang, Mi Zhang, Junjie Sun, Chenyue Wang, and Min Yang, *Fudan University;* Hui Xue, Jialing Tao, Ranjie Duan, and Jiexi Liu, *Alibaba Group*

"I Cannot Write This Because It Violates Our Content Policy": Understanding Content Moderation Policies and User Experiences in Generative AI Products 3727
Lan Gao, Oscar Chen, Rachel Lee, Nick Feamster, Chenhao Tan, and Marshini Chetty, *University of Chicago*

Are CAPTCHAs Still Bot-hard? Generalized Visual CAPTCHA Solving with Agentic Vision Language Model . . .3747
Xiwen Teoh, *Shanghai Jiao Tong University; National University of Singapore;* Yun Lin, *Shanghai Jiao Tong University;* Siqi Li and Ruofan Liu, *National University of Singapore;* Avi Sollomoni and Yaniv Harel, *Tel Aviv University;* Jin Song Dong, *National University of Singapore*

Make Agent Defeat Agent: Automatic Detection of Taint-Style Vulnerabilities in LLM-based Agents 3767
Fengyu Liu, Yuan Zhang, Jiaqi Luo, Jiarun Dai, Tian Chen, Letian Yuan, Zhengmin Yu, Youkun Shi, Ke Li, and Chengyuan Zhou, *Fudan University;* Hao Chen, *UC Davis;* Min Yang, *Fudan University*

Machine Against the RAG: Jamming Retrieval-Augmented Generation with Blocker Documents 3787
Avital Shafran, *The Hebrew University;* Roei Schuster, *Wild Moose;* Vitaly Shmatikov, *Cornell Tech*

Topic-FlipRAG: Topic-Orientated Adversarial Opinion Manipulation Attacks to Retrieval-Augmented Generation Models 3807
Yuyang Gong, Zhuo Chen, Jiawei Liu, Miaokun Chen, Fengchang Yu, and Wei Lu, *Wuhan University;* XiaoFeng Wang, *Nanyang Technological University;* Xiaozhong Liu, *Worcester Polytechnic Institute*

PoisonedRAG: Knowledge Corruption Attacks to Retrieval-Augmented Generation of Large Language Models . . 3827
Wei Zou and Runpeng Geng, *Pennsylvania State University;* Binghui Wang, *Illinois Institute of Technology;* Jinyuan Jia, *Pennsylvania State University*

TracLLM: A Generic Framework for Attributing Long Context LLMs 3845
Yanting Wang, Wei Zou, Runpeng Geng, and Jinyuan Jia, *The Pennsylvania State University*

Hardware Security 2: Signals, Waves, and Side-Channel Secrets

Sound of Interference: Electromagnetic Eavesdropping Attack on Digital Microphones Using Pulse Density Modulation 3865
Arifu Onishi, *The University of Electro-Communications;* S. Hrushikesh Bhupathiraju, Rishikesh Bhatt, and Sara Rampazzi, *University of Florida;* Takeshi Sugawara, *The University of Electro-Communications*

TimeTravel: Real-time Timing Drift Attack on System Time Using Acoustic Waves 3885
Jianshuo Liu and Hong Li, *Institute of Information Engineering, Chinese Academy of Sciences;* Haining Wang, *Virginia Tech;* Mengjie Sun, Hui Wen, Jinfa Wang, and Limin Sun, *Institute of Information Engineering, Chinese Academy of Sciences*

DiskSpy: Exploring a Long-Range Covert-Channel Attack via mmWave Sensing of μm-level HDD Vibrations. . . . 3903
Weiye Xu, *Zhejiang University; China Mobile Research Institute;* Danli Wen, *Zhejiang University;* Jianwei Liu, *Zhejiang University; Hangzhou City University;* Zixin Lin, *Zhejiang University;* Yuanqing Zheng, *The Hong Kong Polytechnic University;* Xian Xu and Jinsong Han, *Zhejiang University*

HubBub: Contention-Based Side-Channel Attacks on USB Hubs. 3921
Junpeng Wan, *Purdue University;* Yanxiang Bi, *The Chinese University of Hong Kong;* Han Gao and Dave (Jing) Tian, *Purdue University*

Lost in Translation: Enabling Confused Deputy Attacks on EDA Software with TransFuzz 3941
Flavien Solt and Kaveh Razavi, *ETH Zurich*

Automated Discovery of Semantic Attacks in Multi-Robot Navigation Systems 3959
Doguhan Yeke and Kartik A. Pant, *Purdue University;* Muslum Ozgur Ozmen, *Arizona State University;* Hyungsub Kim, *Indiana University Bloomington;* James M. Goppert, Inseok Hwang, Antonio Bianchi, and Z. Berkay Celik, *Purdue University*

The Ghost Navigator: Revisiting the Hidden Vulnerability of Localization in Autonomous Driving 3979
Junqi Zhang, *University of Science and Technology of China;* Shaoyin Cheng, *University of Science and Technology of China and Anhui Province Key Laboratory of Cyberspace Security Situation Awareness and Evaluation;* Linqing Hu, *University of Science and Technology of China;* Jie Zhang, *CFAR and IHPC, A*STAR;* Chengyu Shi, *DeepBlue College;* Xingshuo Han and Tianwei Zhang, *Nanyang Technological University;* Yueqiang Cheng, *MediaTek;* Weiming Zhang, *University of Science and Technology of China and Anhui Province Key Laboratory of Digital Security*

NeuroScope: Reverse Engineering Deep Neural Network on Edge Devices using Dynamic Analysis 3999
Ruoyu Wu and Muqi Zou, *Purdue University;* Arslan Khan and Taegyu Kim, *Pennsylvania State University;* Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi, *Purdue University*

BarraCUDA: Edge GPUs do Leak DNN Weights 4017
Peter Horvath, *Radboud University;* Lukasz Chmielewski, *Masaryk University, Radboud University;* Léo Weissbart and Lejla Batina, *Radboud University;* Yuval Yarom, *Ruhr University Bochum*

Blockchain Security 2: Infrastructure, Protocol Design, and Governance

CollisionRepair: First-Aid and Automated Patching for Storage Collision Vulnerabilities in Smart Contracts . . . 4035
Yu Pan and Wanjing Han, *University of Utah;* Yue Duan, *Singapore Management University;* Mu Zhang, *University of Utah*

On the Atomicity and Efficiency of Blockchain Payment Channels 4053
Di Wu, Shoupeng Ren, and Yuman Bai, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University;* Lipeng He, *University of Waterloo;* Jian Liu, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University;* Wu Wen, *International Business School, Zhejiang University;* Kui Ren and Chun Chen, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University*

Parallelizing Universal Atomic Swaps for Multi-Chain Cryptocurrency Exchanges 4073
Danlei Xiao, Chuan Zhang, and Haotian Deng, *Beijing Institute of Technology;* Jinwen Liang, *The Hong Kong Polytechnic University;* Licheng Wang and Liehuang Zhu, *Beijing Institute of Technology*

Automated Soundness and Completeness Vetting of Polygon zkEVM 4093
Xinghao Peng, *The Hong Kong Polytechnic University;* Zhiyuan Sun, *The Hong Kong Polytechnic University and Southern University of Science and Technology;* Kunsong Zhao, Zuchao Ma, Zihao Li, Jinan Jiang, and Xiapu Luo, *The Hong Kong Polytechnic University;* Yinqian Zhang, *Southern University of Science and Technology*

Does Finality Gadget Finalize Your Block? A Case Study of Binance Consensus. 4109
Rujia Li, *Tsinghua University;* Jingyuan Ding, *Shandong University;* Qin Wang, *CSIRO Data61;* Keting Jia, *Tsinghua University;* Haibin Zhang, *Yangtze Delta Region Institute of Tsinghua University;* Sisi Duan, *Tsinghua University*

Following Devils' Footprint: Towards Real-time Detection of Price Manipulation Attacks. 4127
Bosi Zhang, *Huazhong University of Science and Technology;* Ningyu He, *The Hong Kong Polytechnic University;* Xiaohui Hu, Kai Ma, and Haoyu Wang, *Huazhong University of Science and Technology*

Recover from Excessive Faults in Partially-Synchronous BFT SMR 4147
Tiantian Gong and Gustavo Franco Camilo, *Purdue University;* Kartik Nayak, *Duke University;* Andrew Lewis-Pye, *London School of Economics;* Aniket Kate, *Purdue University and Supra Research*

TockOwl: Asynchronous Consensus with Fault and Network Adaptability. 4167
Minghang Li and Qianhong Wu, *Beihang University;* Zhipeng Wang, *Imperial College London;* Bo Qin, *Renmin University of China;* Bohang Wei, Hang Ruan, Shihong Xiong, and Zhenyang Ding, *Beihang University*

Thunderdome: Timelock-Free Rationally-Secure Virtual Channels 4187
Zeta Avarikioti, *TU Wien & Common Prefix;* Yuheng Wang, *TU Wien;* Yuyi Wang, *CRRC Zhuzhou Institute & Tengen Intelligence Institute*

System Security 3: Mobile Platforms

The Doom of Device Drivers: Your Android Device (Most Likely) has N-Day Kernel Vulnerabilities 4205
Lukas Maar, *Graz University of Technology;* Florian Draschbacher, *Graz University of Technology and A-SIT Austria;* Lorenz Schumm, Ernesto Martínez García, and Stefan Mangard, *Graz University of Technology*

NASS: Fuzzing All Native Android System Services with Interface Awareness and Coverage 4225
Philipp Mao, Marcel Busch, and Mathias Payer, *EPFL*

Ariadne: Navigating through the Labyrinth of Data-Driven Customization Inconsistencies in Android 4245
Parjanya Vyas, Haseeb Ur Rehman Faheem, Yousra Aafer, and N. Asokan, *University of Waterloo*

Harness: Transparent and Lightweight Protection of Vehicle Control on Untrusted Android Automotive Operating System 4265
Haochen Gong, Siyu Hong, Shenyi Yang, Rui Chang, Wenbo Shen, Ziqi Yuan, Chenyang Yu, and Yajin Zhou, *Zhejiang University*

Scoop: Mitigation of Recapture Attacks on Provenance-Based Media Authentication 4285
Yuxin (Myles) Liu, Habiba Farrukh, and Ardalan Amiri Sani, *UC Irvine;* Sharad Agarwal, *Microsoft;* Gene Tsudik, *UC Irvine*

Chimera: Creating Digitally Signed Fake Photos by Fooling Image Recapture and Deepfake Detectors 4305
Seongbin Park, Alexander Vilesov, Jinghuai Zhang, Hossein Khalili, Yuan Tian, Achuta Kadambi, and Nader Sehatbakhsh, *University of California, Los Angeles*

Principled and Automated Approach for Investigating AR/VR Attacks 4325
Muhammad Shoaib, Alex Suh, and Wajih Ul Hassan, *University of Virginia*

***Tracking You from a Thousand Miles Away!* Turning a Bluetooth Device into an Apple AirTag Without Root Privileges. 4345**
Junming Chen, Xiaoyue Ma, Lannan Luo, and Qiang Zeng, *George Mason University*

ChoiceJacking: Compromising Mobile Devices through Malicious Chargers like a Decade ago 4363
Florian Draschbacher, *Graz University of Technology and A-SIT Austria;* Lukas Maar, Mathias Oberhuber, and Stefan Mangard, *Graz University of Technology*

Software Security 2: Patching and Repair

PatchAgent: A Practical Program Repair Agent Mimicking Human Expertise 4381
Zheng Yu, Ziyi Guo, Yuhang Wu, and Jiahao Yu, *Northwestern University;* Meng Xu, *University of Waterloo;* Dongliang Mu, *Independent Researcher;* Yan Chen and Xinyu Xing, *Northwestern University*

Logs In, Patches Out: Automated Vulnerability Repair via Tree-of-Thought LLM Analysis 4401
Youngjoon Kim and Sunguk Shin, *Korea University;* Hyoungshick Kim, *Sungkyunkwan University;* Jiwon Yoon, *Korea University*

SoK: Automated Vulnerability Repair: Methods, Tools, and Assessments 4421
Yiwei Hu, Zhen Li, Kedie Shu, Shenghua Guan, and Deqing Zou, *Huazhong University of Science and Technology;* Shouhuai Xu, *University of Colorado Colorado Springs;* Bin Yuan and Hai Jin, *Huazhong University of Science and Technology*

SoK: Towards Effective Automated Vulnerability Repair 4441
Ying Li, *University of California, Los Angeles;* Faysal Hossain Shezan, *University of Texas at Arlington;* Bomin Wei, *University of California, Los Angeles;* Gang Wang, *University of Illinois Urbana-Champaign;* Yuan Tian, *University of California, Los Angeles*

VulcanBoost: Boosting ReDoS Fixes through Symbolic Representation and Feature Normalization 4463
Yeting Li and Yecheng Sun, *Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences;* Zhiwu Xu, *College of Computer Science and Software Engineering, Shenzhen University;* Haiming Chen, *Institute of Software, Chinese Academy of Sciences;* Xinyi Wang, Hengyu Yang, and Huina Chao, *Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences;* Cen Zhang, *School of Computer Science and Engineering, Nanyang Technological University;* Yang Xiao, Yanyan Zou, Feng Li, and Wei Huo, *Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences*

Appatch: Automated Adaptive Prompting Large Language Models for Real-World Software Vulnerability Patching 4481
Yu Nong, *University at Buffalo;* Haoran Yang, *Washington State University;* Long Cheng, *Clemson University;* Hongxin Hu and Haipeng Cai, *University at Buffalo*

RangeSanitizer: Detecting Memory Errors with Efficient Range Checks 4501
Floris Gorter and Cristiano Giuffrida, *Vrije Universiteit Amsterdam*

DisPatch: Unraveling Security Patches from Entangled Code Changes 4521
Shiyu Sun and Yunlong Xing, *George Mason University;* Xinda Wang, *University of Texas at Dallas;* Shu Wang, *Palo Alto Networks, Inc.;* Qi Li, *Tsinghua University;* Kun Sun, *George Mason University*

Attacker Control and Bug Prioritization 4541
Guilhem Lacombe and Sébastien Bardin, *Université Paris-Saclay, CEA, List, France*

ML and AI Security 2

VoiceWukong: Benchmarking Deepfake Voice Detection. 4561
Ziwei Yan, Yanjie Zhao, and Haoyu Wang, *Huazhong University of Science and Technology*

SafeSpeech: Robust and Universal Voice Protection Against Malicious Speech Synthesis. 4581
Zhisheng Zhang, *Beijing University of Posts and Telecommunications;* Derui Wang, *CSIRO's Data61;* Qianyi Yang, Pengyang Huang, and Junhan Pu, *Beijing University of Posts and Telecommunications;* Yuxin Cao, *National University of Singapore;* Kai Ye, *The University of Hong Kong;* Jie Hao and Yixian Yang, *Beijing University of Posts and Telecommunications*

Audio Watermark: Dynamic and Harmless Watermark for Black-box Voice Dataset Copyright Protection 4601
Hanqing Guo, *University of Hawaii at Mānoa;* Junfeng Guo, *University of Maryland;* Bocheng Chen and Yuanda Wang, *Michigan State University;* Xun Chen, *Samsung Research America;* Heng Huang, *University of Maryland;* Qiben Yan and Li Xiao, *Michigan State University*

SoK: Automated TTP Extraction from CTI Reports – Are We There Yet?. 4621
Marvin Büchel, *Carl von Ossietzky Universität Oldenburg;* Tommaso Paladini, *Politecnico di Milano, NEC Laboratories Europe GmbH;* Stefano Longari, Michele Carminati, and Stefano Zanero, *Politecnico di Milano;* Hodaya Binyamini, Gal Engelberg, and Dan Klein, *Accenture Labs;* Giancarlo Guizzardi, *University of Twente;* Marco Caselli, *Siemens AG;* Andrea Continella and Maarten van Steen, *University of Twente;* Andreas Peter, *Carl von Ossietzky Universität Oldenburg;* Thijs van Ede, *University of Twente*

Whispering Under the Eaves: Protecting User Privacy Against Commercial and LLM-powered Automatic Speech Recognition Systems 4643
Weifei Jin, *Beijing University of Posts and Telecommunications;* Yuxin Cao, *National University of Singapore;* Junjie Su, *Beijing University of Posts and Telecommunications;* Derui Wang, *CSIRO's Data61;* Yedi Zhang, *National University of Singapore;* Minhui Xue, *CSIRO's Data61;* Jie Hao, *Beijing University of Posts and Telecommunications;* Jin Song Dong, *National University of Singapore;* Yixian Yang, *Beijing University of Posts and Telecommunications*

AudioMarkNet: Audio Watermarking for Deepfake Speech Detection 4663
Wei Zong, Yang-Wai Chow, Willy Susilo, and Joonsang Baek, *University of Wollongong;* Seyit Camtepe, *CSIRO Data61*

SoK: Efficiency Robustness of Dynamic Deep Learning Systems. 4683
Ravishka Rathnasuriya, Tingxi Li, Zexin Xu, Zihe Song, Mirazul Haque, Simin Chen, and Wei Yang, *The University of Texas at Dallas*

From Meme to Threat: On the Hateful Meme Understanding and Induced Hateful Content Generation in Open-Source Vision Language Models. 4703
Yihan Ma, Xinyue Shen, and Yiting Qu, *CISPA Helmholtz Center for Information Security;* Ning Yu, *Netflix Eyeline Studios;* Michael Backes, *CISPA Helmholtz Center for Information Security;* Savvas Zannettou, *Delft University of Technology;* Yang Zhang, *CISPA Helmholtz Center for Information Security*

When Translators Refuse to Translate: A Novel Attack to Speech Translation Systems. 4723
Haolin Wu, *Wuhan University and Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, China;* Chang Liu, *University of Science and Technology of China;* Jing Chen, Ruiying Du, Kun He, and Yu Zhang, *Wuhan University and Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, China;* Cong Wu and Tianwei Zhang, *Nanyang Technological University;* Qing Guo and Jie Zhang, *CFAR and IHPC, A*STAR, Singapore*

Fraud, Malware, Spam

MalGuard: Towards Real-Time, Accurate, and Actionable Detection of Malicious Packages in PyPI Ecosystem . . .4741
Xingan Gao, Xiaobing Sun, and Sicong Cao, *Yangzhou University;* Kaifeng Huang, *Tongji University;* Di Wu, *University of Southern Queensland;* Xiaolei Liu, *China Academy of Engineering Physics;* Xingwei Lin, *Zhejiang University;* Yang Xiang, *Swinburne University of Technology*

VAPD: An Anomaly Detection Model for PDF Malware Forensics with Adversarial Robustness 4759
Side Liu, *Wuhan University;* Jiang Ming, *Tulane University;* Yilin Zhou, Jianming Fu, and Guojun Peng, *Wuhan University*

NOKEScam: Understanding and Rectifying Non-Sense Keywords Spear Scam in Search Engines 4779
Mingxuan Liu, *Zhongguancun Laboratory;* Yunyi Zhang, *Tsinghua University and National University of Defense Technology;* Lijie Wu, *Tsinghua University;* Baojun Liu, *Tsinghua University and Zhongguancun Laboratory;* Geng Hong, *Fudan University;* Yiming Zhang, *Tsinghua University;* Hui Jiang, *Tsinghua University and Baidu Inc;* Jia Zhang and Haixin Duan, *Tsinghua University and Quancheng Laboratory;* Min Zhang, *National University of Defense Technology;* Wei Guan, *Baidu Inc;* Fan Shi, *National University of Defense Technology;* Min Yang, *Fudan University*

The Ransomware Decade: The Creation of a Fine-Grained Dataset and a Longitudinal Study 4799
Armin Sarabi, Ziyuan Huang, Chenlan Wang, Tai Karir, and Mingyan Liu, *University of Michigan*

High Stakes, Low Certainty: Evaluating the Efficacy of High-Level Indicators of Compromise in Ransomware Attribution 4819
Max van der Horst, *Delft University of Technology;* Ricky Kho, *Sogeti;* Olga Gadyatskaya, *Leiden University;* Michel Mollema, *Northwave Cybersecurity;* Michel Van Eeten and Yury Zhauniarovich, *Delft University of Technology*

DarkGram: A Large-Scale Analysis of Cybercriminal Activity Channels on Telegram 4839
Sayak Saha Roy and Elham Pourabbas Vafa, *The University of Texas at Arlington;* Kobra Khanmohamaddi, *Sheridan College;* Shirin Nilizadeh, *The University of Texas at Arlington*

"Please don't send that bot anything": A Mixed-methods Study of Personal Impersonation Attacks Targeting Digital Payments on Social Media 4859
Hoang Dai Nguyen, *Louisiana State Univeristy;* Sumit Dhungana, Madhulika Itha, and Phani Vadrevu, *Louisiana State University*

'Hey mum, I dropped my phone down the toilet': Investigating Hi Mum and Dad SMS Scams in the United Kingdom 4879
Sharad Agarwal, *University College London* (*UCL*)*, Stop Scams UK;* Emma Harvey, *Stop Scams UK;* Enrico Mariconti, *University College London* (*UCL*)*;* Guillermo Suarez-Tangil, *IMDEA Networks Institute;* Marie Vasek, *University College London* (*UCL*)

Fighting Fire with Fire: Continuous Attack for Adversarial Android Malware Detection 4897
Yinyuan Zhang, *School of Computer Science, Peking University; Key Laboratory of High Confidence Software Technologys* (*Peking University*)*, Ministry of Education;* Cuiying Gao, *Huazhong University of Science and Technology; JD.com;* Yueming Wu, *Nanyang Technological University;* Shihan Dou, *Fudan University;* Cong Wu, *Nanyang Technological University;* Ying Zhang, *Key Laboratory of High Confidence Software Technologys* (*Peking University*)*, Ministry of Education; National Engineering Research Center of Software Engineering, Peking University;* Wei Yuan, *Huazhong University of Science and Technology;* Yang Liu, *Nanyang Technological University*

Crypto 3: Formal Methods and Private Computation

Hobbit: Space-Efficient zkSNARK with Optimal Prover Time 4917
Christodoulos Pappas and Dimitrios Papadopoulos, *The Hong Kong University of Science and Technology*

A Tale of Two Worlds, a Formal Story of WireGuard Hybridization 4937
Pascal Lafourcade and Dhekra Mahmoud, *Université Clermont Auvergne, CNRS, Clermont Auvergne INP, Mines Saint-Etienne, LIMOS, 63000 Clermont-Ferrand, France;* Sylvain Ruhault and Abdul Rahman Taleb, *Agence Nationale de la Sécurité des Systèmes d'Information* (*ANSSI*)*, France*

Improved Secure Two-party Computation from a Geometric Perspective 4957
Hao Guo, *School of Science and Engineering, The Chinese University of Hong Kong, Shenzhen;* Liqiang Peng, *Alibaba Group;* Haiyang Xue, *Singapore Management University;* Li Peng and Weiran Liu, *Alibaba Group;* Zhe Liu, *Zhejiang Lab;* Lei Hu, *Institute of Information Engineering, Chinese Academy of Sciences*

Secure Caches for Compartmentalized Software 4975
Kerem Arıkan, Huaxin Tang, Williams Zhang Cen, and Yu David Liu, *Binghamton University;* Nael Abu-Ghazaleh, *University of California, Riverside;* Dmitry Ponomarev, *Binghamton University*

zk-promises: Anonymous Moderation, Reputation, and Blocking from Anonymous Credentials with Callbacks. . . 4995
Maurice Shih, Michael Rosenberg, and Hari Kailad, *University Of Maryland;* Ian Miers, *University of Maryland*

A Formal Analysis of Apple's iMessage PQ3 Protocol 5015
Felix Linker, Ralf Sasse, and David Basin, *ETH Zurich*

Towards Practical, End-to-End Formally Verified X.509 Certificate Validators with Verdict 5035
Zhengyao Lin, Michael McLoughlin, and Pratap Singh, *Carnegie Mellon University;* Rory Brennan-Jones, *University of Rochester;* Paul Hitchcox, *Carnegie Mellon University;* Joshua Gancher, *Northeastern University;* Bryan Parno, *Carnegie Mellon University*

PICACHV: Formally Verified Data Use Policy Enforcement for Secure Data Analytics 5053
Haobin Hiroki Chen and Hongbo Chen, *Indiana University Bloomington;* Mingshen Sun, *Independent Researcher;* Chenghong Wang, *Indiana University Bloomington;* XiaoFeng Wang, *Nanyang Technological University*

OwlC: Compiling Security Protocols to Verified, Secure, High-Performance Libraries 5071
Pratap Singh, *Carnegie Mellon University;* Joshua Gancher, *Northeastern University;* Bryan Parno, *Carnegie Mellon University*

Friday, August 15

Social Issues and Security

On the Virtues of Information Security in the UK Climate Movement 5091
Mikaela Brough and Rikke Bjerg Jensen, *Royal Holloway, University of London;* Martin R. Albrecht, *King's College London*

Tracking the Takes and Trajectories of English-Language News Narratives across Trustworthy and Worrisome Websites 5111
Hans W. A. Hanley, Emily Okabe, and Zakir Durumeric, *Stanford University*

"No, I Can't Be a Security Personnel on Your Phone": Security and Privacy Threats From Sharing Infrastructure in Rural Ghana 5131
Emmanuel Tweneboah, *Max Planck Institute for Security and Privacy;* Collins W. Munyendo, *Max Planck Institute for Security and Privacy and The George Washington University;* Yixin Zou, *Max Planck Institute for Security and Privacy*

Regulating Smart Device Support Periods: User Expectations and the European Cyber Resilience Act 5149
Lorenz Kustosch and Carlos Gañán, *Delft University of Technology;* Mattis van 't Schip, *Radboud University;* Michel van Eeten and Simon Parkin, *Delft University of Technology*

Characterizing the MrDeepFakes Sexual Deepfake Marketplace 5169
Catherine Han and Anne Li, *Stanford University;* Deepak Kumar, *University of California, San Diego;* Zakir Durumeric, *Stanford University*

Vulnerability of Text-Matching in ML/AI Conference Reviewer Assignments to Collusions. 5189
Jhih-Yi (Janet) Hsieh, Aditi Raghunathan, and Nihar B. Shah, *Carnegie Mellon University*

DORMANT: Defending against Pose-driven Human Image Animation 5209
Jiachen Zhou and Mingsi Wang, *Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China;* Tianlin Li, *Nanyang Technological University, Singapore;* Guozhu Meng and Kai Chen, *Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China*

The Conspiracy Money Machine: Uncovering Telegram's Conspiracy Channels and their Profit Model 5229
Vincenzo Imperati, Massimo La Morgia, Alessandro Mei, Alberto Maria Mongardini, and Francesco Sassi, *Sapienza University of Rome*

SoK: Machine Learning for Misinformation Detection 5247
Madelyne Xiao and Jonathan Mayer, *Princeton University*

Network Security 3: BLE and Cellular

LLFUZZ: An Over-the-Air Dynamic Testing Framework for Cellular Baseband Lower Layers 5267
Tuan Dinh Hoang and Taekkyung Oh, *KAIST;* CheolJun Park, *Kyung Hee University;* Insu Yun and Yongdae Kim, *KAIST*

CORECRISIS: Threat-Guided and Context-Aware Iterative Learning and Fuzzing of 5G Core Networks 5287
Yilu Dong, Tianchang Yang, Abdullah Al Ishtiaq, Syed Md Mukit Rashid, Ali Ranjbar, Kai Tu, Tianwei Wu, Md Sultan Mahmud, and Syed Rafiul Hussain, *The Pennsylvania State University*

GLaDoS: Location-aware Denial-of-Service of Cellular Networks 5307
Simon Erni and Martin Kotuliak, *ETH Zurich;* Richard Baker and Ivan Martinovic, *University of Oxford;* Srdjan Capkun, *ETH Zurich*

AKMA+: Security and Privacy-Enhanced and Standard-Compatible AKMA for 5G Communication 5327
Yang Yang and Guomin Yang, *Singapore Management University;* Yingjiu Li, *University of Oregon;* Minming Huang, *Singapore Management University;* Zilin Shen and Imtiaz Karim, *Purdue University;* Ralf Sasse and David Basin, *ETH Zurich;* Elisa Bertino, *Purdue University;* Jian Weng, *Jinan University;* Hwee Hwa PANG and Robert H. Deng, *Singapore Management University*

A Thorough Security Analysis of BLE Proximity Tracking Protocols 5347
Xiaofeng Liu, *School of Cyber Science and Technology, Shandong University;* Chaoshun Zuo, *Ohio State University;* Qinsheng Hou, *School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University;* Pengcheng Ren, *China Mobile Information Technology Co., Ltd.;* Jianliang Wu, *Simon Fraser University;* Qingchuan Zhao, *City University of Hong Kong;* Shanqing Guo, *School of Cyber Science and Technology, Shandong University & Shandong Key Laboratory of Artificial Intelligence Security*

Gotta Detect 'Em All: Fake Base Station and Multi-Step Attack Detection in Cellular Networks 5365
Kazi Samin Mubasshir, Imtiaz Karim, and Elisa Bertino, *Purdue University*

SNI5GECT: A Practical Approach to Inject aNRchy into 5G NR 5385
Shijie Luo, Matheus Garbelini, Sudipta Chattopadhyay, and Jianying Zhou, *Singapore University of Technology and Design*

Preventing Artificially Inflated SMS Attacks through Large-Scale Traffic Inspection 5405
Jun Ho Huh, Hyejin Shin, Sunwoo Ahn, and Hayoon Yi, *Samsung Research;* Joonho Cho, Taewoo Kim, Minchae Lim, and Nuel Choi, *Samsung Electronics*

eSIMplicity or eSIMplification? Privacy and Security Risks in the eSIM Ecosystem 5425
Maryam Motallebighomi, Jason Veara, Evangelos Bitsikas, and Aanjhan Ranganathan, *Northeastern University*

ML and AI Privacy 2

Disparate Privacy Vulnerability: Targeted Attribute Inference Attacks and Defenses 5445
Ehsanul Kabir, Lucas Craig, and Shagufta Mehnaz, *Pennsylvania State University*

Enhanced Label-Only Membership Inference Attacks with Fewer Queries 5465
Hao Li, *Institute of Software, Chinese Academy of Sciences;* Zheng Li, *Shandong University;* Siyuan Wu, Yutong Ye, Min Zhang, and Dengguo Feng, *Institute of Software, Chinese Academy of Sciences;* Yang Zhang, *CISPA Helmholtz Center for Information Security*

For Human Ears Only: Preventing Automated Monitoring on Voice Data 5485
Irtaza Shahid and Nirupam Roy, *University of Maryland, College Park*

Towards a Re-evaluation of Data Forging Attacks in Practice 5505
Mohamed Suliman, *IBM Research and Trinity College Dublin, The University of Dublin;* Anisa Halimi, Swanand Ravindra Kadhe, and Nathalie Baracaldo, *IBM Research;* Douglas Leith, *Trinity College Dublin, The University of Dublin*

Free Record-Level Privacy Risk Evaluation Through Artifact-Based Methods 5525
Joseph Pollock, Igor Shilov, Euodia Dodd, and Yves-Alexandre de Montjoye, *Imperial College London*

Rectifying Privacy and Efficacy Measurements in Machine Unlearning: A New Inference Attack Perspective . . . 5545
Nima Naderloui and Shenao Yan, *University of Connecticut;* Binghui Wang, *Illinois Institute of Technology;* Jie Fu and Wendy Hui Wang, *Stevens Institute of Technology;* Weiran Liu, *Alibaba Group;* Yuan Hong, *University of Connecticut*

Phantom: Privacy-Preserving Deep Neural Network Model Obfuscation in Heterogeneous TEE and GPU System 5565
Juyang Bai, *Johns Hopkins University;* Md Hafizul Islam Chowdhuryy, *University of Central Florida;* Jingtao Li, *Sony AI;* Fan Yao, *University of Central Florida;* Chaitali Chakrabarti and Deliang Fan, *Arizona State University*

LOHEN: Layer-wise Optimizations for Neural Network Inferences over Encrypted Data with High Performance *or* Accuracy 5583
Kevin Nam, Youyeon Joo, Dongju Lee, and Seungjin Ha, *Seoul National University;* Hyunyoung Oh, *Gachon University;* Hyungon Moon, *UNIST;* Yunheung Paek, *Seoul National University*

SoK: Data Reconstruction Attacks Against Machine Learning Models: Definition, Metrics, and Benchmark. . . . 5601
Rui Wen, *Institute of Science Tokyo;* Yiyong Liu, Michael Backes, and Yang Zhang, *CISPA Helmholtz Center for Information Security*

Hardware Security 3: Side-Channel and Fault Injection Attacks

McSee: Evaluating Advanced Rowhammer Attacks and Defenses via Automated DRAM Traffic Analysis. 5621
Patrick Jattke and Michele Marazzi, *ETH Zurich;* Flavien Solt, *UC Berkeley;* Max Wipfli, Stefan Gloor, and Kaveh Razavi, *ETH Zurich*

Not so Refreshing: Attacking GPUs using RFM Rowhammer Mitigation 5641
Ravan Nazaraliyev and Yicheng Zhang, *University of California, Riverside;* Sankha Baran Dutta, *Brookhaven National Laboratory;* Andres Marquez and Kevin Barker, *Pacific Northwest National Laboratory;* Nael Abu-Ghazaleh, *University of California, Riverside*

Posthammer: Pervasive Browser-based Rowhammer Attacks with Postponed Refresh Commands 5661
Finn de Ridder, Patrick Jattke, and Kaveh Razavi, *ETH Zurich*

ECC.fail: Mounting Rowhammer Attacks on DDR4 Servers with ECC Memory. 5679
Nureddin Kamadan and Walter Wang, *Georgia Tech;* Stephan van Schaik, *University of Michigan;* Christina Garman, *Purdue University;* Daniel Genkin, *Georgia Tech;* Yuval Yarom, *Ruhr University Bochum*

Relocate-Vote: Using Sparsity Information to Exploit Ciphertext Side-Channels. 5699
Yuqin Yan, *University of Toronto;* Wei Huang, *University of Toronto and Seneca Polytechnic;* Ilya Grishchenko and Gururaj Saileshwar, *University of Toronto;* Aastha Mehta, *University of British Columbia;* David Lie, *University of Toronto*

GPUHammer: Rowhammer Attacks on GPU Memories are Practical 5719
Chris S. Lin, Joyce Qu, and Gururaj Saileshwar, *University of Toronto*

SCASE: Automated Secret Recovery via Side-Channel-Assisted Symbolic Execution 5739
Daniel Weber, Lukas Gerlach, and Leon Trampert, *CISPA Helmholtz Center for Information Security;* Youheng Lü, *SCHUTZWERK GmbH;* Jo Van Bulck, *DistriNet, KU Leuven;* Michael Schwarz, *CISPA Helmholtz Center for Information Security*

Shadows in Cipher Spaces: Exploiting Tweak Repetition in Hardware Memory Encryption 5759
Wei Peng, Yinshuai Li, and Yinqian Zhang, *Southern University of Science and Technology*

Breaking the Blindfold: Deep Learning-based Blind Side-channel Analysis. 5777
Azade Rezaeezade, *Delft University of Technology and Digital Security Group, Radboud University;* Trevor Yap, Dirmanto Jap, and Shivam Bhasin, *Temasek Laboratories and National integrated Centre For Evaluation, Nanyang Technological University;* Stjepan Picek, *Digital Security Group, Radboud University and University of Zagreb Faculty of Electrical Engineering and Computing*

Privacy 2: Consent, Compliance, and Provable Privacy

Evaluating Privacy Policies under Modern Privacy Laws At Scale: An LLM-Based Automated Approach 5797
Qinge Xie, Karthik Ramakrishnan, and Frank Li, *Georgia Institute of Technology*

Navigating Cookie Consent Violations Across the Globe 5817
Brian Tang, Duc Bui, and Kang G. Shin, *University of Michigan*

Websites' Global Privacy Control Compliance at Scale and over Time 5837
Katherine Hausladen, Oliver Wang, and Sophie Eng, *Wesleyan University;* Jocelyn Wang, *Princeton University;* Francisca Wijaya, Matthew May, and Sebastian Zimmeck, *Wesleyan University*

Privacy Law Enforcement Under Centralized Governance: A Qualitative Analysis of Four Years' Special Privacy Rectification Campaigns 5857
Tao Jing, *School of Cyber Science and Engineering, Huazhong University of Science and Technology, JinYinHu Laboratory, Hubei Key Laboratory of Distributed System Security, Hubei Engineering Research Center on Big Data Security;* Yao Li and Jingzhou Ye, *University of Central Florida;* Jie Wang, *School of Cyber Science and Engineering, Huazhong University of Science and Technology, JinYinHu Laboratory, Hubei Key Laboratory of Distributed System Security, Hubei Engineering Research Center on Big Data Security;* Xueqiang Wang, *University of Central Florida*

A Stakeholder-Based Framework to Highlight Tensions when Implementing Privacy Features 5875
Julia Netter, Tim Nelson, Skyler Austen, Eva Lau, Colton Rusch, Malte Schwarzkopf, and Kathi Fisler, *Brown University*

Who Pays Whom? Anonymous EMV-Compliant Contactless Payments 5893
Charles Olivier-Anclin, *Universite de Clermont Auvergne, LIMOS; INSA CVL, LIFO, Université d'Orléans, Inria; and be ys Pay;* Ioana Boureanu, Liqun Chen, and C. J. P. Newton, *Surrey Centre for Cyber Security, University of Surrey;* Tom Chothia, Anna Clee, and Andreas Kokkinis, *University of Birmingham;* Pascal Lafourcade, *Universite de Clermont Auvergne, LIMOS*

ATKSCOPES: Multiresolution Adversarial Perturbation as a Unified Attack on Perceptual Hashing and Beyond . . . 5913
Yushu Zhang, Yuanyuan Sun, and Shuren Qi, *Nanjing University of Aeronautics and Astronautics;* Zhongyun Hua, *Harbin Institute of Technology, Shenzhen;* Wenying Wen and Yuming Fang, *Jiangxi University of Finance and Economics*

SPEECHGUARD: Recoverable and Customizable Speech Privacy Protection 5931
Jingmiao Zhang, Suyuan Liu, Jiahui Hou, Zhiqiang Wang, Haikuo Yu, and Xiang-Yang Li, *University of Science and Technology of China*

Shimmer: a Provably Secure Steganography Based on Entropy Collecting Mechanism 5949
Minhao Bai, Kaiyi Pang, Guorui Liao, Jinshuai Yang, and Yongfeng Huang, *Tsinghua University*

Usable Privacy and Security 3

How Transparent is Usable Privacy and Security Research? A Meta-Study on Current Research Transparency Practices 5967
Jan H. Klemmer, Juliane Schmüser, Fabian Fischer, Jacques Suray, Jan-Ulrich Holtgrave, and Simon Lenau, *CISPA Helmholtz Center for Information Security;* Byron M. Lowens, *Indiana University Indianapolis;* Florian Schaub, *University of Michigan;* Sascha Fahl, *CISPA Helmholtz Center for Information Security*

Understanding How Users Prepare for and React to Smartphone Theft 5987
Divyanshu Bhardwaj and Sumair Ijaz Hashmi, *CISPA Helmholtz Center for Information Security, Saarland University;* Katharina Krombholz and Maximilian Golla, *CISPA Helmholtz Center for Information Security*

Exploring User Security and Privacy Attitudes and Concerns Toward the Use of General-Purpose LLM Chatbots for Mental Health 6007
Jabari Kwesi, Jiaxun Cao, Riya Manchanda, and Pardis Emami-Naeini, *Duke University*

Investigating the Impact of Online Community Involvement on Safety Practices and Perceived Risks Among People Who Use Drugs 6025
Jiliang Li and Nora Sinong Lu, *Xi'an Jiaotong University;* Isaak Hanimann, *ETH Zurich;* Janice Jianing Si, *University of Macau;* Dazhao Cheng, *WuHan University;* Xiaobo Zhou and Kanye Ye Wang, *University of Macau*

Privacy Solution or Menace? Investigating Perceptions of Radio-Frequency Sensing 6045
Maximiliane Windl, *LMU Munich/Munich Center for Machine Learning (MCML);* Omer Akgul, *Carnegie Mellon University/ RSAC Labs;* Nathan Malkin, *New Jersey Institute of Technology;* Lorrie Faith Cranor, *Carnegie Mellon University*

Navigating Security and Privacy Threats in Homeless Service Provision 6065
Yuxi Wu, *Northeastern University;* Ruoxi Zhang, Shiyue Liu, Mufei He, and Aidan Hong, *Carnegie Mellon University;* Jeremy J. Northup, *Point Park University;* Calla Kainaroi, *Bridge to the Mountains;* Fei Fang and Hong Shen, *Carnegie Mellon University*

Security and Privacy Advice for UPI Users in India 6085
Deepthi Mungara and Harshini Sri Ramulu, *Paderborn University;* Yasemin Acar, *Paderborn University and The George Washington University*

"Helps me Take the Post With a Grain of Salt:" Soft Moderation Effects on Accuracy Perceptions and Sharing Intentions of Inauthentic Political Content on X 6105
Filipo Sharevski, *DePaul University;* Verena Distler, *Aalto University;* Florian Alt, *Ludwig Maximilians Universität, University of the Bundeswehr Munich*

As Advertised? Understanding the Impact of Influencer VPN Ads 6125
Omer Akgul, *University of Maryland/Carnegie Mellon University;* Richard Roberts, Emma Shroyer, Dave Levin, and Michelle L. Mazurek, *University of Maryland*

Software Security 3: Fuzzing

Fuzzing the PHP Interpreter via Dataflow Fusion 6143
Yuancheng Jiang, Chuqi Zhang, Bonan Ruan, Jiahao Liu, Manuel Rigger, Roland H. C. Yap, and Zhenkai Liang, *National University of Singapore*

WALTZZ: WebAssembly Runtime Fuzzing with Stack-Invariant Transformation 6159
Lingming Zhang, *Zhejiang University;* Binbin Zhao, *Zhejiang University, Georgia Institute of Technology, and Engineering Research Center of Blockchain Application, Supervision And Management* (*Southeast University*), *Ministry of Education;* Jiacheng Xu and Peiyu Liu, *Zhejiang University;* Qinge Xie, *Georgia Institute of Technology;* Yuan Tian, *UCLA;* Jianhai Chen and Shouling Ji, *Zhejiang University*

MBFuzzer: A Multi-Party Protocol Fuzzer for MQTT Brokers 6179
Xiangpu Song, *Shandong University;* Jianliang Wu, *Simon Fraser University;* Yingpei Zeng, *Hangzhou Dianzi University;* Hao Pan, *Shandong University;* Chaoshun Zuo, *Ohio State University;* Qingchuan Zhao, *City University of Hong Kong;* Shanqing Guo, *Shandong University and Shandong Key Laboratory of Artificial Intelligence Security*

CHAINFUZZ: Exploiting Upstream Vulnerabilities in Open-Source Supply Chains 6199
Peng Deng, Lei Zhang, Yuchuan Meng, Zhemin Yang, Yuan Zhang, and Min Yang, *Fudan University*

IDFUZZ: Intelligent Directed Grey-box Fuzzing 6219
Yiyang Chen, *Tsinghua University;* Chao Zhang, *Tsinghua University and JCSS, Tsinghua University* (*INSC*) - *Science City* (*Guangzhou*) *Digital Technology Group Co., Ltd.;* Long Wang, *Tsinghua University;* Wenyu Zhu, *Tsinghua University and AscendGrace Tech;* Changhua Luo, *Wuhan University;* Nuoqi Gui, Zheyu Ma, and Xingjian Zhang, *Tsinghua University;* Bingkai Su, *Hunan University*

Robust, Efficient, and Widely Available Greybox Fuzzing for COTS Binaries with System Call Pattern Feedback. . . .6239
Jifan Xiao, *Key Laboratory of High Confidence Software Technologies, Peking University;* Peng Jiang, *Southeast University;* Zixi Zhao, Ruizhe Huang, Junlin Liu, and Ding Li, *Key Laboratory of High Confidence Software Technologies, Peking University*

BLuEMan: A Stateful Simulation-based Fuzzing Framework for Open-Source RTOS Bluetooth Low Energy Protocol Stacks 6259
Wei-Che Kao, Yen-Chia Chen, Yu-Sheng Lin, Yu-Cheng Yang, Chi-Yu Li, and Chun-Ying Huang, *National Yang Ming Chiao Tung University*

ELFUZZ: Efficient Input Generation via LLM-driven Synthesis Over Fuzzer Space 6279
Chuyang Chen, *The Ohio State University;* Brendan Dolan-Gavitt, *New York University;* Zhiqiang Lin, *The Ohio State University*

Hybrid Language Processor Fuzzing via LLM-Based Constraint Solving 6299
Yupeng Yang, Shenglong Yao, Jizhou Chen, and Wenke Lee, *Georgia Institute of Technology*

ML and AI Security 3: Backdoors, Poisoning, Unlearning

Rowhammer-Based Trojan Injection: One Bit Flip Is Sufficient for Backdooring DNNs 6319
Xiang Li, Ying Meng, Junming Chen, Lannan Luo, and Qiang Zeng, *George Mason University*

From Purity to Peril: Backdooring Merged Models From "Harmless" Benign Components 6339
Lijin Wang, *The Hong Kong University of Science and Technology* (*Guangzhou*); Jingjing Wang, *Zhejiang University;* Tianshuo Cong, *Tsinghua University;* Xinlei He, *The Hong Kong University of Science and Technology* (*Guangzhou*); Zhan Qin, *Zhejiang University;* Xinyi Huang, *Jinan University*

Revisiting Training-Inference Trigger Intensity in Backdoor Attacks 6359
Chenhao Lin, Chenyang Zhao, Shiwei Wang, Longtian Wang, Chao Shen, and Zhengyu Zhao, *Xi'an Jiaotong University*

Persistent Backdoor Attacks in Continual Learning 6379
Zhen Guo, Abhinav Kumar, and Reza Tourani, *Saint Louis University*

Data Duplication: A Novel Multi-Purpose Attack Paradigm in Machine Unlearning 6399
Dayong Ye, *University of Technology Sydney;* Tianqing Zhu, *City University of Macau;* Jiayang Li, Kun Gao, and Bo Liu, *University of Technology Sydney;* Leo Yu Zhang, *Griffith University;* Wanlei Zhou, *City University of Macau;* Yang Zhang, *CISPA Helmholtz Center for Information Security*

DeBackdoor: A Deductive Framework for Detecting Backdoor Attacks on Deep Models with Limited Data 6419
Dorde Popovic and Amin Sadeghi, *Qatar Computing Research Institute, Hamad Bin Khalifa University;* Ting Yu, *Mohamed bin Zayed University of Artificial Intelligence;* Sanjay Chawla and Issa Khalil, *Qatar Computing Research Institute, Hamad Bin Khalifa University*

SoK: Gradient Inversion Attacks in Federated Learning. 6439
Vincenzo Carletti, Pasquale Foggia, Carlo Mazzocca, Giuseppe Parrella, and Mario Vento, *University of Salerno*

PoiSAFL: Scalable Poisoning Attack Framework to Byzantine-resilient Semi-asynchronous Federated Learning . . .6461
Xiaoyi Pang, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University; Hangzhou High-Tech Zone* (*Binjiang*) *Institute of Blockchain and Data Security;* Chenxu Zhao, *The State Key Laboratory of Blockchain and Data Security and School of Cyber Science and Technology, Zhejiang University;* Zhibo Wang, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University; Hangzhou High-Tech Zone* (*Binjiang*) *Institute of Blockchain and Data Security;* Jiahui Hu, *The State Key Laboratory of Blockchain and Data Security and School of Cyber Science and Technology, Zhejiang University;* Yinggui Wang, Lei Wang, and Tao Wei, *Ant Group;* Kui Ren and Chun Chen, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University; Hangzhou High-Tech Zone* (*Binjiang*) *Institute of Blockchain and Data Security*

Towards Lifecycle Unlearning Commitment Management: Measuring Sample-level Unlearning Completeness . . . 6481
Cheng-Long Wang, *King Abdullah University of Science and Technology;* Qi Li, *King Abdullah University of Science and Technology and National University of Singapore;* Zihang Xiang, *King Abdullah University of Science and Technology;* Yinzhi Cao, *Johns Hopkins University;* Di Wang, *King Abdullah University of Science and Technology*

Privacy 3: Attacks

Addressing the Address Books' (Interdependent) Privacy Issues 6501
Kavous Salehzadeh Niksirat, *University of Lausanne / Max Planck Institute for Security and Privacy;* Lev Velykoivanenko, *University of Lausanne;* Samuel Mätzler, *University of Zurich;* Stephan Mulders, *Maastricht University;* Aurelia Tamò-Larrieux, Marc-Olivier Boldi, Mathias Humbert, and Kévin Huguenin, *University of Lausanne*

HyTrack: Resurrectable and Persistent Tracking Across Android Apps and the Web 6521
Malte Wessels, Simon Koch, Jan Drescher, Louis Bettels, David Klein, and Martin Johns, *TU Braunschweig*

I Can Tell Your Secrets: Inferring Privacy Attributes from Mini-app Interaction History in Super-apps 6541
Yifeng Cai, *Peking University;* Ziqi Zhang, *University of Illinois Urbana-Champaign;* Mengyu Yao and Junlin Liu, *Peking University;* Xiaoke Zhao, Xinyi Fu, Ruoyu Li, and Zhe Li, *Ant Group;* Xiangqun Chen, Yao Guo, and Ding Li, *Peking University*

Seeing Through: Analyzing and Attacking Virtual Backgrounds in Video Calls 6561
Felix Weissberg, *BIFOLD & TU Berlin;* Jan Malte Hilgefort and Steve Grogorick, *TU Braunschweig;* Daniel Arp, *TU Wien;* Thorsten Eisenhofer, *BIFOLD & TU Berlin;* Martin Eisemann, *TU Braunschweig;* Konrad Rieck, *BIFOLD & TU Berlin*

Endangered Privacy: Large-Scale Monitoring of Video Streaming Services 6581
Martin Björklund and Romaric Duvignau, *Chalmers University of Technology and University of Gothenburg*

Bots can Snoop: Uncovering and Mitigating Privacy Risks of Bots in Group Chats. 6599
Kai-Hsiang Chou, Yi-Min Lin, Yi-An Wang, and Jonathan Weiping Li, *National Taiwan University;* Tiffany Hyun-Jin Kim, *HRL Laboratories;* Hsu-Chun Hsiao, *National Taiwan University and Academia Sinica*

EchoLLM: LLM-Augmented Acoustic Eavesdropping Attack on Bone Conduction Headphones with mmWave Radar. 6619
Xin Yao and Kecheng Huang, *Central South University;* Yimin Chen, *University of Massachusetts Lowell;* Jiawei Guo, Jie Tang, and Ming Zhao, *Central South University*

DiffLoc: WiFi Hidden Camera Localization Based on Electromagnetic Diffraction. 6639
Xiang Zhang, *University of Science and Technology of China;* Jie Zhang, *CFAR and IHPC, A*STAR;* Huan Yan, *Guizhou Normal University;* Jinyang Huang, *Hefei University of Technology;* Zehua Ma and Bin Liu, *University of Science and Technology of China;* Meng Li, *Hefei University of Technology;* Kejiang Chen, *University of Science and Technology of China;* Qing Guo, *CFAR and IHPC, A*STAR;* Tianwei Zhang, *Nanyang Technological University;* Zhi Liu, *The University of Electro-Communications*

Double-Edged Shield: On the Fingerprintability of Customized Ad Blockers 6659
Saiid El Hajj Chehade, *EPFL;* Ben Stock, *CISPA Helmholtz Center for Information Security;* Carmela Troncoso, *EPFL and Max-Planck Institute for Security and Privacy* (*MPI-SP*)

Crypto 4: Systems and Protocols

Encrypted Access Logging for Online Accounts: Device Attributions without Device Tracking 6679
Carolina Ortega Pérez and Alaa Daffalla, *Cornell University;* Thomas Ristenpart, *Cornell Tech*

Exploring How to Authenticate Application Messages in MLS: More Efficient, Post-Quantum, and Anonymous Blocklistable 6699
Keitaro Hashimoto, *National Institute of Advanced Industrial Science and Technology* (*AIST*)*;* Shuichi Katsumata, *National Institute of Advanced Industrial Science and Technology* (*AIST*) *and PQShield;* Guillermo Pascual-Perez, *Institute of Science and Technology Austria* (*ISTA*)

How to Compare Bandwidth Constrained Two-Party Secure Messaging Protocols: A Quest for A More Efficient and Secure Post-Quantum Protocol 6717
Benedikt Auerbach, *PQShield;* Yevgeniy Dodis and Daniel Jost, *New York University;* Shuichi Katsumata, *PQShield and AIST;* Rolfe Schmidt, *Signal Messenger*

S/MINE: Collecting and Analyzing S/MIME Certificates at Scale 6737
Gurur Öndarö and Jonas Kaspereit, *Münster University of Applied Sciences;* Samson Umezulike, *Fraunhofer SIT and National Research Center for Applied Cybersecurity ATHENE;* Christoph Saatjohann, *Münster University of Applied Sciences;* Fabian Ising, *Fraunhofer SIT and National Research Center for Applied Cybersecurity ATHENE;* Sebastian Schinzel, *Münster University of Applied Sciences, Fraunhofer SIT and National Research Center for Applied Cybersecurity ATHENE*

Achilles: A Formal Framework of Leaking Secrets from Signature Schemes via Rowhammer 6757
Junkai Liang, *Peking University;* Zhi Zhang, *The University of Western Australia;* Xin Zhang and Qingni Shen, *Peking University;* Yansong Gao, *The University of Western Australia;* Xingliang Yuan, *The University of Melbourne;* Haiyang Xue and Pengfei Wu, *Singapore Management University;* Zhonghai Wu, *Peking University*

Bundled Authenticated Key Exchange: A Concrete Treatment of Signal's Handshake Protocol and Post-Quantum Security 6777
Keitaro Hashimoto, *National Institute of Advanced Industrial Science and Technology* (*AIST*)*;* Shuichi Katsumata, *National Institute of Advanced Industrial Science and Technology* (*AIST*) *and PQShield;* Thom Wiggers, *PQShield*

Comprehensive Deniability Analysis of Signal Handshake Protocols: X3DH, PQXDH to Fully Post-Quantum with Deniable Ring Signatures 6797
Shuichi Katsumata, *PQShield & AIST;* Guilhem Niot, *PQShield & Univ Rennes, CNRS, IRISA;* Ida Tucker and Thom Wiggers, *PQShield*

SparSamp: Efficient Provably Secure Steganography Based on Sparse Sampling 6817
Yaofei Wang, *Hefei University of Technology;* Gang Pei, *Hefei University Of Technology;* Kejiang Chen and Jinyang Ding, *University of Science and Technology of China;* Chao Pan, Weilong Pang, and Donghui Hu, *Hefei University of Technology;* Weiming Zhang, *University of Science and Technology of China*

A Framework for Designing Provably Secure Steganography 6837
Guorui Liao, Jinshuai Yang, Weizhi Shao, and Yongfeng Huang, *Tsinghua University*

Software Security 4: Fuzzing and Other Software Analysis

RevDecode: Enhancing Binary Function Matching with Context-Aware Graph Representations and Relevance Decoding 6857
Tongwei Ren, Ronghan Che, and Guin R. Gilman, *Worcester Polytechnic Institute;* Lorenzo De Carli, *University of Calgary;* Robert J. Walls, *Worcester Polytechnic Institute*

BLens: Contrastive Captioning of Binary Functions using Ensemble Embedding 6877
Tristan Benoit, *Ludwig-Maximilians-Universität München and Bundeswehr University Munich;* Yunru Wang, Moritz Dannehl, and Johannes Kinder, *Ludwig-Maximilians-Universität München and Munich Center for Machine Learning*

TRex: Practical Type Reconstruction for Binary Code 6897
Jay Bosamiya, *Microsoft Research;* Maverick Woo and Bryan Parno, *Carnegie Mellon University*

Vest: Verified, Secure, High-Performance Parsing and Serialization for Rust 6917
Yi Cai, *University of Maryland, College Park;* Pratap Singh and Zhengyao Lin, *Carnegie Mellon University;* Jay Bosamiya, *Microsoft Research;* Joshua Gancher, *Northeastern University;* Milijana Surbatovich, *University of Maryland, College Park;* Bryan Parno, *Carnegie Mellon University*

LEMIX: Enabling Testing of Embedded Applications as Linux Applications 6937
Sai Ritvik Tanksalkar, Siddharth Muralee, Srihari Danduri, Paschal Amusuo, Antonio Bianchi, James C. Davis, and Aravind Kumar Machiry, *Purdue University*

TYPEPULSE: Detecting Type Confusion Bugs in Rust Programs. 6957
Hung-Mao Chen and Xu He, *George Mason University;* Shu Wang, *George Mason University and Palo Alto Networks, Inc.;* Xiaokuan Zhang and Kun Sun, *George Mason University*

From Alarms to Real Bugs: Multi-target Multi-step Directed Greybox Fuzzing for Static Analysis Result Verification 6977
Andrew Bao, *University of Minnesota, Twin Cities;* Wenjia Zhao, *Xi'an Jiaotong University;* Yanhao Wang, *Independent Researcher;* Yueqiang Cheng, *MediaTek;* Stephen McCamant and Pen-Chung Yew, *University of Minnesota, Twin Cities*

Low-Cost and Comprehensive Non-textual Input Fuzzing with LLM-Synthesized Input Generators. 6999
Kunpeng Zhang, Zongjie Li, Daoyuan Wu, and Shuai Wang, *The Hong Kong University of Science and Technology;* Xin Xia, *Zhejiang University*

Pig in a Poke: Automatically Detecting and Exploiting Link Following Vulnerabilities in Windows File Operations . . .7019
Bocheng Xiang, Yuan Zhang, Fengyu Liu, Hao Huang, Zihan Lin, and Min Yang, *Fudan University*

Network Security 4: Internet and Beyond

GNSS-WASP: GNSS Wide Area SPoofing. 7039
Christopher Tibaldo, Harshad Sathaye, Giovanni Camurati, and Srdjan Capkun, *ETH Zurich, Switzerland*

LEO-Range: Physical Layer Design for Secure Ranging with Low Earth Orbiting Satellites. 7059
Daniele Coppola, *ETH Zurich;* Arslan Mumtaz, *CISPA – Helmholtz Center for Information Security;* Giovanni Camurati and Harshad Sathaye, *ETH Zurich;* Mridula Singh, *CISPA – Helmholtz Center for Information Security;* Srdjan Capkun, *ETH Zurich*

A Comprehensive Formal Security Analysis of OPC UA 7077
Vincent Diemunsch, *ANSSI and Université de Lorraine, CNRS, Inria, LORIA, France;* Lucca Hirschi and Steve Kremer, *Université de Lorraine, CNRS, Inria, LORIA, France*

Towards Internet-Based State Learning of TLS State Machines 7097
Marcel Maehren and Nurullah Erinola, *Ruhr University Bochum;* Robert Merget, *Technology Innovation Institute;* Jörg Schwenk, *Ruhr University Bochum;* Juraj Somorovsky, *Paderborn University*

Misty Registry: An Empirical Study of Flawed Domain Registry Operation 7117
Mingming Zhang, *Zhongguancun Laboratory;* Yunyi Zhang, *National University of Defense Technology and Tsinghua University;* Baojun Liu and Haixin Duan, *Tsinghua University and Zhongguancun Laboratory;* Min Zhang, Fan Shi, and Chengxi Xu, *National University of Defense Technology*

Haunted by Legacy: Discovering and Exploiting Vulnerable Tunnelling Hosts 7135
Angelos Beitis and Mathy Vanhoef, *DistriNet, KU Leuven*

GeCos Replacing Experts: Generalizable and Comprehensible Industrial Intrusion Detection 7153
Konrad Wolsing, Eric Wagner, and Luisa Lux, *Fraunhofer FKIE and RWTH Aachen University;* Klaus Wehrle, *RWTH Aachen University;* Martin Henze, *RWTH Aachen University and Fraunhofer FKIE*

ORTHRUS: Achieving High Quality of Attribution in Provenance-based Intrusion Detection Systems 7173
Baoxiang Jiang, *Xi'an Jiaotong University;* Tristan Bilot, *Université Paris-Saclay, LISITE– Isep, and Iriguard;* Nour El Madhoun, *LISITE – Isep;* Khaldoun Al Agha, *Université Paris-Saclay;* Anis Zouaoui, *Iriguard;* Shahrear Iqbal, *National Research Council Canada;* Xueyuan Han, *Wake Forest University;* Thomas Pasquier, *University of British Columbia*

Sometimes Simpler is Better: A Comprehensive Analysis of State-of-the-Art Provenance-Based Intrusion Detection Systems 7193
Tristan Bilot, *Université Paris-Saclay, LISITE, Isep, and Iriguard;* Baoxiang Jiang, *Xi'an Jiaotong University;* Zefeng Li, *University of British Columbia;* Nour El Madhoun, *LISITE, Isep;* Khaldoun Al Agha, *Université Paris-Saclay;* Anis Zouaoui, *Iriguard;* Thomas Pasquier, *University of British Columbia*

ML and AI Security 4: Robustness

CAMP in the Odyssey: Provably Robust Reinforcement Learning with Certified Radius Maximization 7213
Derui Wang, Kristen Moore, Diksha Goel, and Minjune Kim, *CSIRO's Data61 and Cyber Security Cooperative Research Centre;* Gang Li, Yang Li, and Robin Doss, *Deakin University;* Minhui Xue, *CSIRO's Data61 and Cyber Security Cooperative Research Centre;* Bo Li, *University of Chicago;* Seyit Camtepe, *CSIRO's Data61 and Cyber Security Cooperative Research Centre;* Liming Zhu, *CSIRO's Data61*

Towards Understanding and Enhancing Security of Proof-of-Training for DNN Model Ownership Verification . 7233
Yijia Chang and Hanrui Jiang, *The Hong Kong University of Science and Technology* (*Guangzhou*)*;* Chao Lin, *Fujian Normal University;* Xinyi Huang and Jian Weng, *Jinan University*

AGNNCert: Defending Graph Neural Networks against Arbitrary Perturbations with Deterministic Certification . . .7251
Jiate Li and Binghui Wang, *Illinois Institute of Technology*

LightShed: Defeating Perturbation-based Image Copyright Protections 7271
Hanna Foerster, *University of Cambridge;* Sasha Behrouzi and Phillip Rieger, *Technical University of Darmstadt;* Murtuza Jadliwala, *University of Texas at San Antonio;* Ahmad-Reza Sadeghi, *Technical University of Darmstadt*

Robustifying ML-powered Network Classifiers with PANTS 7291
Minhao Jin and Maria Apostolaki, *Princeton University*

THEMIS: Towards Practical Intellectual Property Protection for Post-Deployment On-Device Deep Learning Models 7311
Yujin Huang, *The University of Melbourne;* Zhi Zhang, *The University of Western Australia;* Qingchuan Zhao, *City University of Hong Kong;* Xingliang Yuan, *The University of Melbourne;* Chunyang Chen, *Technical University of Munich*

A Crack in the Bark: Leveraging Public Knowledge to Remove Tree-Ring Watermarks 7331
Junhua Lin and Marc Juarez, *University of Edinburgh*

CertTA: Certified Robustness Made Practical for Learning-Based Traffic Analysis 7349
Jinzhu Yan, *Tsinghua University;* Zhuotao Liu, *Tsinghua University and Zhongguancun Laboratory;* Yuyang Xie, *Tsinghua University;* Shiyu Liang, *Shanghai Jiao Tong University;* Lin Liu, *National University of Defense Technology;* Ke Xu, *Tsinghua University and Zhongguancun Laboratory*

Invisible but Detected: Physical Adversarial Shadow Attack and Defense on LiDAR Object Detection 7369
Ryunosuke Kobayashi, *Waseda University;* Kazuki Nomoto, *Waseda University and Deloitte Tohmatsu Cyber LLC;* Yuna Tanaka and Go Tsuruoka, *Waseda University;* Tatsuya Mori, *Waseda University and NICT and RIKEN AIP*

From Threat to Trust: Exploiting Attention Mechanisms for Attacks and Defenses in Cooperative Perception . . 7387
Chenyi Wang, *University of Arizona;* Raymond Muller and Ruoyu Song, *Purdue University;* Jean-Philippe Monteuuis and Jonathan Petit, *Qualcomm;* Yanmao Man, *Independent Researcher, U.S.;* Ryan Gerdes, *Virginia Tech;* Z. Berkay Celik, *Purdue University;* Ming Li, *University Of Arizona*

System Security 4: Kernel and Low-Level System Security

Await() a Second: Evading Control Flow Integrity by Hijacking C++ Coroutines 7407
Marcos Bajo and Christian Rossow, *CISPA Helmholtz Center for Information Security*

System Register Hijacking: Compromising Kernel Integrity By Turning System Registers Against the System . . .7427
Jennifer Miller, Manas Ghandat, Kyle Zeng, Hongkai Chen, Abdelouahab (Habs) Benchikh, Tiffany Bao, Ruoyu Wang, Adam Doupé, and Yan Shoshitaishvili, *Arizona State University*

When Good Kernel Defenses Go Bad: Reliable and Stable Kernel Exploits via Defense-Amplified TLB Side-Channel Leaks 7447
Lukas Maar, Lukas Giner, Daniel Gruss, and Stefan Mangard, *Graz University of Technology*

Approximation Enforced Execution of Untrusted Linux Kernel Extensions 7467
Hao Sun and Zhendong Su, *ETH Zurich*

EKC: A Portable and Extensible Kernel Compartment for De-Privileging Commodity OS 7487
Jiaqin Yan, *Shanghai Jiao Tong University, Southern University of Science and Technology;* Qiujiang Chen, Shuai Zhou, and Yuke Peng, *Southern University of Science and Technology;* Guoxing Chen, *Shanghai Jiao Tong University;* Yinqian Zhang, *Southern University of Science and Technology*

The Cost of Performance: Breaking ThreadX with Kernel Object Masquerading Attacks. 7507
Xinhui Shao and Zhen Ling, *Southeast University;* Yue Zhang, *Drexel University;* Huaiyu Yan and Yumeng Wei, *Southeast University;* Lan Luo and Zixia Liu, *Anhui University of Technology;* Junzhou Luo, *Southeast University;* Xinwen Fu, *University of Massachusetts Lowell*

Finding Metadata Inconsistencies in Distributed File Systems via Cross-Node Operation Modeling 7525
Fuchen Ma, Yuanliang Chen, Yuanhang Zhou, and Zhen Yan, *Tsinghua University;* Hao Sun, *ETH Zurich;* Yu Jiang, *Tsinghua University*

Save what must be saved: Secure context switching with Sailor 7545
Neelu S. Kalani, *EPFL and IBM Research - Zurich;* Thomas Bourgeat, *EPFL;* Guerney D. H. Hunt, *IBM T. J. Watson Research Center;* Wojciech Ozga, *IBM Research - Zurich*

Privacy 4: Privacy-Preserving Computation

Flexway O-Sort: Enclave-Friendly and Optimal Oblivious Sorting 7563
Tianyao Gu, *Carnegie Mellon University and Oblivious Labs Inc.;* Yilei Wang, *Alibaba Cloud;* Afonso Tinoco, *Carnegie Mellon University and Oblivious Labs Inc.;* Bingnan Chen and Ke Yi, *HKUST;* Elaine Shi, *Carnegie Mellon University and Oblivious Labs Inc*.

Treebeard: A Scalable and Fault Tolerant ORAM Datastore 7583
Amin Setayesh, Cheran Mahalingam, Emily Chen, and Sujaya Maiyya, *University of Waterloo*

Learning from Functionality Outputs: Private Join and Compute in the Real World 7603
Francesca Falzon, *ETH Zürich;* Tianxin Tang, *Eindhoven University of Technology*

ALERT: Machine Learning-Enhanced Risk Estimation for Databases Supporting Encrypted Queries 7623
Longxiang Wang, *City University of Hong Kong;* Lei Xu, *Nanjing University of Science and Technology and City University of Hong Kong;* Yufei Chen, *City University of Hong Kong;* Ying Zou, *Nanjing University of Science and Technology;* Cong Wang, *City University of Hong Kong*

Distributed Private Aggregation in Graph Neural Networks. 7643
Huanhuan Jia, Yuanbo Zhao, Kai Dong, Zhen Ling, Ming Yang, and Junzhou Luo, *Southeast University;* Xinwen Fu, *University of Massachusetts Lowell*

Suda: An Efficient and Secure Unbalanced Data Alignment Framework for Vertical Privacy-Preserving Machine Learning. 7663
Lushan Song, *Fudan University and ByteDance;* Qizhi Zhang and Yu Lin, *ByteDance;* Haoyu Niu, *Fudan University;* Daode Zhang, *ByteDance;* Zheng Qu and Weili Han, *Fudan University;* Jue Hong, Quanwei Cai, and Ye Wu, *ByteDance*

Assuring Certified Database Utility in Privacy-Preserving Database Fingerprinting 7683
Mingyang Song and Zhongyun Hua, *Harbin Institute of Technology, Shenzhen;* Yifeng Zheng, *The Hong Kong Polytechnic University;* Tao Xiang, *Chongqing University;* Guoai Xu, *Harbin Institute of Technology, Shenzhen;* Xingliang Yuan, *The University of Melbourne*

Shechi: A Secure Distributed Computation Compiler Based on Multiparty Homomorphic Encryption 7703
Haris Smajlović, *University of Victoria;* David Froelicher, *MIT;* Ariya Shajii, *Exaloop Inc.;* Bonnie Berger, *MIT;* Hyunghoon Cho, *Yale University;* Ibrahim Numanagić, *University of Victoria*

Private Set Intersection and other Set Operations in the Third Party Setting 7723
Foo Yee Yeo and Jason H. M. Ying, *Seagate Technology*

Authentication

Detecting Compromise of Passkey Storage on the Cloud 7743
Mazharul Islam, *University of Wisconsin—Madison;* Sunpreet S. Arora, *Visa Research;* Rahul Chatterjee, *University of Wisconsin—Madison;* Ke Coby Wang, *Visa Research*

OneTouch: Effortless 2FA Scheme to Secure Fingerprint Authentication with Wearable OTP Token 7763
Yihui Yan and Zhice Yang, *ShanghaiTech University*

Practically Secure Honey Password Vaults: New Design and New Evaluation against Online Guessing 7781
Haibo Cheng, Fugeng Huang, and Jiahong Yang, *Peking University;* Wenting Li, *Beijing Institute of Graphic Communication;* Ping Wang, *Peking University*

Password Guessing Using Large Language Models 7799
Yunkai Zou, Maoxiang An, and Ding Wang, *Nankai University*

A Framework for Abusability Analysis: The Case of Passkeys in Interpersonal Threat Models 7819
Alaa Daffalla and Arkaprabha Bhattacharya, *Cornell University;* Jacob Wilder, *Independent Researcher;* Rahul Chatterjee, *University of Wisconsin—Madison;* Nicola Dell, *Cornell Tech;* Rosanna Bellini, *New York University;* Thomas Ristenpart, *Cornell Tech*

CertPHash: Towards Certified Perceptual Hashing via Robust Training 7839
Yuchen Yang and Qichang Liu, *The Johns Hopkins University;* Christopher Brix, *RWTH Aachen University;* Huan Zhang, *University of Illinois at Urbana–Champaign;* Yinzhi Cao, *The Johns Hopkins University*

Phishing Attacks against Password Manager Browser Extensions 7857
Claudio Anliker, Daniele Lain, and Srdjan Capkun, *ETH Zurich*

Red Bleed: A Pragmatic Near-Infrared Presentation Attack on Facial Biometric Authentication Systems. 7877
Bowen Hu, Kuo Wang, and Chip Hong Chang, *Nanyang Technological University*

System Security 5: Securing Systems and Protocols

Oblivious Digital Tokens 7897
Mihael Liskij, *ETH Zurich;* Xuhua Ding, *Singapore Management University;* Gene Tsudik, *UC Irvine;* David Basin, *ETH Zurich*

V-ORAM: A Versatile and Adaptive ORAM Framework with Service Transformation for Dynamic Workloads . . . 7917
Bo Zhang and Helei Cui, *Northwestern Polytechnical University;* Xingliang Yuan, *The University of Melbourne;* Zhiwen Yu, *Northwestern Polytechnical University and Harbin Engineering University;* Bin Guo, *Northwestern Polytechnical University*

AutoVR: Automated UI Exploration for Detecting Sensitive Data Flow Exposures in Virtual Reality Apps 7937
John Y. Kim, Chaoshun Zuo, Yanjie Zhao, and Zhiqiang Lin, *The Ohio State University*

***Found in Translation*: A Generative Language Modeling Approach to Memory Access Pattern Attacks 7957**
Grace Jia, Alex Wong, and Anurag Khandelwal, *Yale University*

More is Less: Extra Features in Contactless Payments Break Security 7977
George Pavlides, *Surrey Centre for Cyber Security, University of Surrey;* Anna Clee, *University of Birmingham;* Ioana Boureanu, *Surrey Centre for Cyber Security, University of Surrey;* Tom Chothia, *University of Birmingham*

Current Affairs: A Security Measurement Study of CCS EV Charging Deployments. 7997
Marcell Szakály, Sebastian Köhler, and Ivan Martinovic, *University of Oxford*

STEK Sharing is Not Caring: Bypassing TLS Authentication in Web Servers using Session Tickets 8017
Sven Hebrok, Tim Leonhard Storm, Felix Matthias Cramer, Maximilian Radoy, and Juraj Somorovsky, *Paderborn University*

Too Much of a Good Thing: (In-)Security of Mandatory Security Software for Financial Services in South Korea 8035
Taisic Yun, *Theori Inc., KAIST;* Suhwan Jeong, *KAIST;* Yonghwa Lee, *Theori Inc.;* Seungjoo Kim, *Korea University;* Hyoungshick Kim, *Sungkyunkwan University;* Insu Yun and Yongdae Kim, *KAIST*

Vulnerabilities in LLMs: Privacy, Safety, and Defense

Unsafe LLM-Based Search: Quantitative Analysis and Mitigation of Safety Risks in AI Web Search 8055
Zeren Luo, Zifan Peng, Yule Liu, and Zhen Sun, *The Hong Kong University of Science and Technology* (*Guangzhou*)*;* Mingchen Li, *The Hong Kong University of Science and Technology* (*Guangzhou*)*; University of North Texas;* Jingyi Zheng and Xinlei He, *The Hong Kong University of Science and Technology* (*Guangzhou*)

Generated Data with Fake Privacy: Hidden Dangers of Fine-tuning Large Language Models on Generated Data . . 8075
Atilla Akkus and Masoud Poorghaffar Aghdam, *Bilkent University;* Mingjie Li, Junjie Chu, Michael Backes, and Yang Zhang, *CISPA Helmholtz Center for Information Security;* Sinem Sav, *Bilkent University*

Cloak, Honey, Trap: Proactive Defenses Against LLM Agents 8095
Daniel Ayzenshteyn, Roy Weiss, and Yisroel Mirsky, *Ben Gurion University of the Negev*

Big Help or Big Brother? Auditing Tracking, Profiling, and Personalization in Generative AI Assistants 8115
Yash Vekaria, *UC Davis;* Aurelio Loris Canino, *UNIRC;* Jonathan Levitsky, *UC Davis;* Alex Ciechonski, *UCL;* Patricia Callejo, *UC3M;* Anna Maria Mandalari, *UCL;* Zubair Shafiq, *UC Davis*

SOFT: Selective Data Obfuscation for Protecting LLM Fine-tuning against Membership Inference Attacks 8135
Kaiyuan Zhang, Siyuan Cheng, Hanxi Guo, Yuetian Chen, Zian Su, Shengwei An, and Yuntao Du, *Purdue University;* Charles Fleming and Ashish Kundu, *Cisco Research;* Xiangyu Zhang and Ninghui Li, *Purdue University*

Effective PII Extraction from LLMs through Augmented Few-Shot Learning 8155
Shuai Cheng, Shu Meng, Haitao Xu, and Haoran Zhang, *The State Key Laboratory of Blockchain and Data Security, Zhejiang University;* Shuai Hao, *Old Dominion University;* Chuan Yue, *Colorado School of Mines;* Wenrui Ma, *Zhejiang Gongshang University;* Meng Han and Fan Zhang, *Zhejiang University;* Zhao Li, *Zhejiang University and Hangzhou Yugu Technology*

Private Investigator: Extracting Personally Identifiable Information from Large Language Models Using Optimized Prompts 8175
Seongho Keum and Dongwon Shin, *KAIST;* Leo Marchyok and Sanghyun Hong, *Oregon State University;* Sooel Son, *KAIST*

PrivacyXray: Detecting Privacy Breaches in LLMs through Semantic Consistency and Probability Certainty . . . 8195
Jinwen He, Yiyang Lu, Zijin Lin, Kai Chen, and Yue Zhao, *Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences*

JBShield: Defending Large Language Models from Jailbreak Attacks through Activated Concept Analysis and Manipulation 8215
Shenyi Zhang and Yuchen Zhai, *Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University;* Keyan Guo and Hongxin Hu, *University at Buffalo;* Shengnan Guo, Zheng Fang, and Lingchen Zhao, *Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University;* Chao Shen, *Xi'an Jiaotong University;* Cong Wang, *City University of Hong Kong;* Qian Wang, *Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University*

Web Security

Web Execution Bundles: Reproducible, Accurate, and Archivable Web Measurements 8235
Florian Hantke, *CISPA Helmholtz Center for Information Security;* Peter Snyder, *Brave Software;* Hamed Haddadi, *Imperial College London and Brave Software;* Ben Stock, *CISPA Helmholtz Center for Information Security*

XSSky: Detecting XSS Vulnerabilities through Local Path-Persistent Fuzzing 8255
Youkun Shi, *Fudan University and The Hong Kong Polytechnic University;* Yuan Zhang, Tianhao Bai, Feng Xue, Jiarun Dai, Fengyu Liu, and Lei Zhang, *Fudan University;* Xiapu Luo, *The Hong Kong Polytechnic University;* Min Yang, *Fudan University*

Zipper: Static Taint Analysis for PHP Applications with Precision and Efficiency 8273
Xinyi Wang and Yeting Li, *{CAS-KLONAT, BKLONSPT}, Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences;* Jie Lu, *SKLP, Institute of Computing Technology, Chinese Academy of Sciences;* Shizhe Cui, *School of Informatics, The University of Edinburgh;* Chenghang Shi, *SKLP, Institute of Computing Technology, Chinese Academy of Sciences and School of Computer Science and Technology, University of Chinese Academy of Sciences;* Qin Mai, *{CAS-KLONAT, BKLONSPT}, Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences;* Yunpei Zhang, *School of Information and Software Engineering, UESTC;* Yang Xiao, Feng Li, and Wei Huo, *{CAS-KLONAT, BKLONSPT}, Institute of Information Engineering, Chinese Academy of Sciences and School of Cyber Security, University of Chinese Academy of Sciences*

The DOMino Effect: Detecting and Exploiting DOM Clobbering Gadgets via Concolic Execution with Symbolic DOM 8293
Zhengyu Liu, Theo Lee, Jianjia Yu, Zifeng Kang, and Yinzhi Cao, *Johns Hopkins University*

FIXX: FInding eXploits from eXamples 8313
Neil P Thimmaiah, Yashashvi J Dave, Rigel Gjomemo, and V.N. Venkatakrishnan, *University of Illinois Chicago*

Careless Retention and Management: Understanding and Detecting Data Retention Denial-of-Service Vulnerabilities in Java Web Containers 8329
Keke Lian, Lei Zhang, and Haoran Zhao, *Fudan University;* Yinzhi Cao, *Johns Hopkins University;* Yongheng Liu, Fute Sun, Yuan Zhang, and Min Yang, *Fudan University*

Effective Directed Fuzzing with Hierarchical Scheduling for Web Vulnerability Detection 8349
Zihan Lin, Yuan Zhang, Jiarun Dai, Xinyou Huang, Bocheng Xiang, Guangliang Yang, Letian Yuan, Lei Zhang, Fengyu Liu, Tian Chen, and Min Yang, *Fudan University*

Towards Automatic Detection and Exploitation of Java Web Application Vulnerabilities via Concolic Execution guided by Cross-thread Object Manipulation 8367
Xinyou Huang, Lei Zhang, Yongheng Liu, and Peng Deng, *Fudan University;* Yinzhi Cao, *Johns Hopkins University;* Yuan Zhang and Min Yang, *Fudan University*

Crypto 5: HE, MPC, Oblivious Computation

Efficient Batchable Secure Outsourced Computation: Depth-Aware Arithmetization of Common Primitives for BFV & BGV 8385
Jelle Vos, *Delft University of Technology;* Mauro Conti, *University of Padua & Delft University of Technology;* Zekeriya Erkin, *Delft University of Technology*

Arbitrary-Threshold Fully Homomorphic Encryption with Lower Complexity 8403
Yijia Chang, *The Hong Kong University of Science and Technology;* Songze Li, *Southeast University*

Leuvenshtein: Efficient FHE-based Edit Distance Computation with Single Bootstrap per Cell 8423
Wouter Legiest and Jan-Pieter D'Anvers, *COSIC, KU Leuven;* Bojan Spasic and Nam-Luc Tran, *Society for Worldwide Interbank Financial Telecommunication* (*Swift*)*;* Ingrid Verbauwhede, *COSIC, KU Leuven*

Engorgio: An Arbitrary-Precision Unbounded-Size Hybrid Encrypted Database via Quantized Fully Homomorphic Encryption 8441
Song Bian, Haowen Pan, Jiaqi Hu, Zhou Zhang, and Yunhao Fu, *Beihang University;* Jiafeng Hua, *Huawei Technology;* Yi Chen and Bo Zhang, *Beijing Academy of Blockchain and Edge Computing;* Yier Jin, *University of Science and Technology of China;* Jin Dong, *Beijing Academy of Blockchain and Edge Computing;* Zhenyu Guan, *Beihang University*

Qelect: Lattice-based Single Secret Leader Election Made Practical 8461
Yunhao Wang and Fan Zhang, *Yale University*

GlitchFHE: Attacking Fully Homomorphic Encryption Using Fault Injection 8481
Lakshmi Likhitha Mankali and Mohammed Nabeel, *Tandon School of Engineering, New York University;* Faiq Raees, *New York University;* Michail Maniatakos, Ozgur Sinanoglu, and Johann Knechtel, *New York University Abu Dhabi*

H_2O_2RAM: A High-Performance Hierarchical Doubly Oblivious RAM 8501
Leqian Zheng, *City University of Hong Kong;* Zheng Zhang, *ByteDance Inc.;* Wentao Dong, *City University of Hong Kong;* Yao Zhang and Ye Wu, *ByteDance Inc.;* Cong Wang, *City University of Hong Kong*

OBLIVIATOR: OBLIVIous Parallel Joins and other OperATORs in Shared Memory Environments 8521
Apostolos Mavrogiannakis, *University of California, Santa Cruz;* Xian Wang, *The Hong Kong University of Science and Technology;* Ioannis Demertzis, *University of California, Santa Cruz;* Dimitrios Papadopoulos, *The Hong Kong University of Science and Technology;* Minos Garofalakis, *ATHENA Research Center and Technical University of Crete*

Efficient Ranking, Order Statistics, and Sorting under CKKS 8541
Federico Mazzone, *University of Twente;* Maarten Everts, *University of Twente and Linksight;* Florian Hahn, *University of Twente;* Andreas Peter, *Carl von Ossietzky Universität Oldenburg*