32nd USENIX Security Symposium  
August 9–11, 2023  
Anaheim, CA, USA

Wednesday, August 9

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

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

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

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

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

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

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

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

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

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

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

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

Squint Hard Enough: Attacking Perceptual Hashing with Adversarial Machine Learning
Jonathan Prokos, Johns Hopkins University; Neil Fendley, Johns Hopkins University Applied Physics Laboratory; Matthew Green, Johns Hopkins University; Roei Schuster, Vector Institute; Eran Tromer, Tel Aviv University and Columbia University; Tushar Jois and Yinzhi Cao, Johns Hopkins University

How to Cover up Anomalous Accesses to Electronic Health Records
Xiaojun Xu, Qingying Hao, Zhuolin Yang, and Bo Li, University of Illinois at Urbana-Champaign; David Liebovitz, Northwestern University; Gang Wang and Carl A. Gunter, University of Illinois at Urbana-Champaign

Kenku: Towards Efficient and Stealthy Black-box Adversarial Attacks against ASR Systems
Xinghui Wu, Xi'an Jiaotong University; Shiqing Ma, University of Massachusetts Amherst; Chao Shen and Chenhao Lin, Xi'an Jiaotong University; Qian Wang, Wuhan University; Qi Li, Tsinghua University; Yuan Rao, Xi'an Jiaotong University

Tubes Among Us: Analog Attack on Automatic Speaker Identification
Shimaa Ahmed and Yash Wani, University of Wisconsin-Madison; Ali Shahin Shamsabadi, Alan Turing Institute; Mohammad Yaghini, University of Toronto and Vector Institute; Ili Shumailov, Vector Institute and University of Oxford; Nicolas Papernot, University of Toronto and Vector Institute; Kassem Fawaz, University of Wisconsin-Madison

Private Set Operations

Efficient Unbalanced Private Set Intersection Cardinality and User-friendly Privacy-preserving Contact Tracing
Mingli Wu and Tsz Hon Yuen, The University of Hong Kong

Near-Optimal Oblivious Key-Value Stores for Efficient PSI, PSU and Volume-Hiding Multi-Maps
Alexander Bienstock, New York University; Sarvar Patel and Joon Young Seo, Google; Kevin Yeo, Google and Columbia University

Distance-Aware Private Set Intersection
Anrin Chakraborti, Duke University; Giulia Fanti, Carnegie Mellon University; Michael K. Reiter, Duke University

Linear Private Set Union from Multi-Query Reverse Private Membership Test
Cong Zhang, State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences; Yu Chen, School of Cyber Science and Technology, Shandong University; State Key Laboratory of Cryptology; Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University; Weiran Liu, Alibaba Group; Min Zhang, School of Cyber Science and Technology, Shandong University; State Key Laboratory of Cryptology; Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University; Dongdai Lin, State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences

Logs and Auditing

Auditing Frameworks Need Resource Isolation: A Systematic Study on the Super Producer Threat to System Auditing and Its Mitigation
Peng Jiang, Ruizhe Huang, Ding Li, Yao Guo, and Xiangqun Chen, MOE Key Lab of HCST, School of Computer Science, Peking University; Jianhai Luan, Yuxin Ren, and Xinwei Hu, Huawei Technologies

AirTAg: Towards Automated Attack Investigation by Unsupervised Learning with Log Texts
Hailun Ding, Rutgers University; Juan Zhai, University of Massachusetts Amherst; Yuhong Nan, Sun Yat-sen University; Shiqing Ma, University of Massachusetts Amherst

Rethinking System Audit Architectures for High Event Coverage and Synchronous Log Availability
Varun Gandhi, Harvard University; Sarbartha Banerjee, University of Texas at Austin; Aniket Agrawal and Adil Ahmad, Arizona State University; Sangho Lee and Marcus Peinado, Microsoft Research

Improving Logging to Reduce Permission Over-Granting Mistakes
Bingyu Shen, Tianyi Shan, and Yuanyuan Zhou, University of California, San Diego
Fighting the Robots
Diving into Robocall Content with SnorCall ................................................................. 427
Sathvik Prasad, Trevor Dunlap, Alexander Ross, and Bradley Reaves, North Carolina State University

UCBlocker: Unwanted Call Blocking Using Anonymous Authentication .................. 445
Changlai Du and Hexuan Yu, Virginia Tech; Yang Xiao, University of Kentucky; Y. Thomas Hou, Virginia Tech; Angelos D. Keromytis, Georgia Institute of Technology; Wenjing Lou, Virginia Tech

Combating Robocalls with Phone Virtual Assistant Mediated Interaction .................. 463
Sharbani Pandit, Georgia Institute of Technology; Krishanu Sarker, Georgia State University; Roberto Perdisci, University of Georgia and Georgia Institute of Technology; Mustaque Ahamad and Diyi Yang, Georgia Institute of Technology

BotScreen: Trust Everybody, but Cut the Aimbots Yourself ........................................ 481
Minyeop Choi, KAIST; Gihyuk Ko, Cyber Security Research Center at KAIST and Carnegie Mellon University; Sang Kil Cha, KAIST and Cyber Security Research Center at KAIST

Perspectives and Incentives
“If I could do this, I feel anyone could:” The Design and Evaluation of a Secondary Authentication Factor Manager ................................................................. 499
Garrett Smith, Tarun Yadav, and Jonathan Dutson, Brigham Young University; Scott Ruoti, University of Tennessee Knoxville; Kent Seamons, Brigham Young University

Exploring Privacy and Incentives Considerations in Adoption of COVID-19 Contact Tracing Apps ........ 517
Oshrat Ayalon, Max Planck Institute for Software Systems; Dana Turjeman, Reichman University; Elissa M. Redmiles, Max Planck Institute for Software Systems

Exploring Tenants’ Preferences of Privacy Negotiation in Airbnb ............................... 535
Zixin Wang, Zhejiang University; Danny Yuxing Huang, New York University; Yaxing Yao, University of Maryland, Baltimore County

Know Your Cybercriminal: Evaluating Attacker Preferences by Measuring Profile Sales on an Active, Leading Criminal Market for User Impersonation at Scale ........................................ 553
Michele Campobasso and Luca Allodi, Eindhoven University of Technology

Traffic Analysis
HorusEye: A Realtime IoT Malicious Traffic Detection Framework using Programmable Switches. ........ 571
Yutao Dong, Tsinghua Shenzhen International Graduate School, Shenzhen, China; Peng Cheng Laboratory, Shenzhen, China; Qing Li, Peng Cheng Laboratory, Shenzhen, China; Kaidong Wu and Ruoyu Li, Tsinghua Shenzhen International Graduate School, Shenzhen, China; Peng Cheng Laboratory, Shenzhen, China; Dan Zhao, Peng Cheng Laboratory, Shenzhen, China; Gareth Tyson, Hong Kong University of Science and Technology (GZ), Guangzhou, China; Junkun Peng, Yong Jiang, and Shutao Xia, Tsinghua Shenzhen International Graduate School, Shenzhen, China; Peng Cheng Laboratory, Shenzhen, China; Mingwei Xu, Tsinghua University, Beijing, China

Jian Qu, Xiaobo Ma, and Jianfeng Li, Xi’an Jiaotong University; Xiapu Luo, The Hong Kong Polytechnic University; Lei Xue, Sun Yat-sen University; Junjie Zhang, Wright State University; Zhenhua Li, Tsinghua University; Li Feng, Southwest Jiaotong University; Xiaohong Guan, Xi’an Jiaotong University

Subverting Website Fingerprinting Defenses with Robust Traffic Representation ............. 607
Meng Shen, School of Cyberspace Science and Technology, Beijing Institute of Technology; Kexin Ji and Zhenbo Gao, School of Computer Science, Beijing Institute of Technology; Qi Li, Institute for Network Sciences and Cyberspace, Tsinghua University; Liehuang Zhu, School of Cyberspace Science and Technology, Beijing Institute of Technology; Ke Xu, Department of Computer Science and Technology, Tsinghua University

Rosetta: Enabling Robust TLS Encrypted Traffic Classification in Diverse Network Environments with TCP-Aware Traffic Augmentation ........................................ 625
Renjie Xie and Jiahao Cao, Tsinghua University; Enhuan Dong and Mingwei Xu, Tsinghua University and Quan Cheng Laboratory; Kun Sun, George Mason University; Qi Li and Licheng Shen, Tsinghua University; Menghao Zhang, Tsinghua University and Kuaishou Technology
Adversarial Patches and Images
Towards Targeted Obfuscation of Adversarial Unsafe Images using Reconstruction and Counterfactual Super Region Attribution Explainability ................................................................. 643
Mazal Bethany, Andrew Seong, Samuel Henrique Silva, Nicole Beebe, Nishant Vishwamitra, and Peyman Najafirad,
The University of Texas at San Antonio

TPatch: A Triggered Physical Adversarial Patch ............................................................... 661
Wenjun Zhu and Xiaoyu Ji, USSLAB, Zhejiang University; Yushi Cheng, BNRist, Tsinghua University; Shibo Zhang and Wenyuan Xu, USSLAB, Zhejiang University

CAPatch: Physical Adversarial Patch against Image Captioning Systems .......................... 679
Shibo Zhang, USSLAB, Zhejiang University; Yushi Cheng, BNRist, Tsinghua University; Wenjun Zhu, Xiaoyu Ji, and Wenyuan Xu, USSLAB, Zhejiang University

Hard-label Black-box Universal Adversarial Patch Attack ................................................ 697
Guanhong Tao, Shengwei An, Siyuan Cheng, Guangyu Shen, and Xiangyu Zhang, Purdue University

Decentralized Finance
Anatomy of a High-Profile Data Breach: Dissecting the Aftermath of a Crypto-Wallet Case .......... 715
Svetlana Abramova and Rainer Böhme, Universität Innsbruck

Glimpse: On-Demand PoW Light Client with Constant-Size Storage for DeFi .......................... 733
Giulia Scaffino, TU Wien and Christian Doppler Laboratory Blockchain Technologies for the Internet of Things; Lukas Aumayr and Zeta Avarikioti, TU Wien; Matteo Maffei, TU Wien and Christian Doppler Laboratory Blockchain Technologies for the Internet of Things

Mixed Signals: Analyzing Ground-Truth Data on the Users and Economics of a Bitcoin Mixing Service ................................................. 751
Fieke Miedema, Kelvin Lubbertsen, Verena Schrama, and Rolf van Wegberg, Delft University of Technology

Is Your Wallet Snitching On You? An Analysis on the Privacy Implications of Web3 .......................... 769
Christof Ferreira Torres, Fiona Willi, and Shweta Shinde, ETH Zurich

Memory
CAPSTONE: A Capability-based Foundation for Trustless Secure Memory Access .................. 787
Jason Zhijingcheng Yu, National University of Singapore; Conrad Watt, University of Cambridge; Aditya Badole, Trevor E. Carlson, and Prateek Saxena, National University of Singapore

FloatZone: Accelerating Memory Error Detection using the Floating Point Unit .................... 805
Floris Gorter, Enrico Barberis, Raphael Iseman, Erik van der Kouwe, Cristiano Giuffrida, and Herbert Bos, Vrije Universiteit Amsterdam

PUMM: Preventing Use-After-Free Using Execution Unit Partitioning .................................. 823
Carter Yagemann, The Ohio State University; Simon P. Chung, Brendan Saltaformaggio, and Wenke Lee, Georgia Institute of Technology

MTSan: A Feasible and Practical Memory Sanitizer for Fuzzing COTS Binaries ..................... 841
Xingman Chen, Tsinghua University; Yinghao Shi, Institute of Information Engineering, Chinese Academy of Sciences; Zheyu Jiang and Yuan Li, Tsinghua University; Ruoyu Wang, Arizona State University; Haixin Duan, Tsinghua University and Zhongguancun Laboratory; Haoyu Wang, Huazhong University of Science and Technology; Chao Zhang, Tsinghua University and Zhongguancun Laboratory

Security in Digital Realities
Hidden Reality: Can Your Hand Gesture Inputs in the Immersive Virtual World are Visible to All? .... 859
Sindhu Reddy Kalathur Gopal and Diksha Shukla, University of Wyoming; James David Wheelock, University of Colorado Boulder; Nitesh Saxena, Texas A&M University, College Station

LocIn: Inferring Semantic Location from Spatial Maps in Mixed Reality ............................. 877
Habiba Farrukh, Reham Mohamed, Aniket Nare, Antonio Bianchi, and Z. Berkay Celik, Purdue University
Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data
Vivek Nair and Wenbo Guo, UC Berkeley; Justus Mattern, RWTH Aachen; Rui Wang and James F. O’Brien, UC Berkeley; Louis Rosenberg, Unanimous AI; Dawn Song, UC Berkeley

Exploring User Reactions and Mental Models Towards Perceptual Manipulation Attacks in Mixed Reality
Kaiming Cheng, Jeffery F. Tian, Tadayoshi Kohno, and Franziska Roesner, University of Washington

Erebus: Access Control for Augmented Reality Systems
Yoonsang Kim, Sanket Goutam, Amir Rahmati, and Arie Kaufman, Stony Brook University

Password Guessing
No Single Silver Bullet: Measuring the Accuracy of Password Strength Meters
Ding Wang, Xuan Shan, and Qiying Dong, Nankai University; Yaosheng Shen, Peking University; Chunfu Jia, Nankai University

Password Guessing Using Random Forest
Ding Wang and Yunkai Zou, Nankai University; Zijian Zhang, Peking University; Kedong Xiu, Nankai University

PASS2EDIT: A Multi-Step Generative Model for Guessing Edited Passwords
Ding Wang and Yunkai Zou, Nankai University; Yuan-An Xiao, Peking University; Siqi Ma, The University of New South Wales; Xiaofeng Chen, Xidian University

Improving Real-world Password Guessing Attacks via Bi-directional Transformers
Ming Xu and Jitao Yu, Fudan University; Xinyi Zhang, Facebook; Chuanwang Wang, Shenghao Zhang, Haoqi Wu, and Weili Han, Fudan University

Araña: Discovering and Characterizing Password Guessing Attacks in Practice
Mazharul Islam, University of Wisconsin–Madison; Marina Sanusi Bohuk, Cornell Tech; Paul Chung, University of Wisconsin–Madison; Thomas Ristenpart, Cornell Tech; Rahul Chatterjee, University of Wisconsin–Madison

Privacy Policies, Labels, Etc.
Poligraph: Automated Privacy Policy Analysis using Knowledge Graphs
Hao Cui, Rahmadi Trimananda, Athina Markopoulou, and Scott Jordan, University of California, Irvine

Calpric: Inclusive and Fine-grain Labeling of Privacy Policies with Crowdsourcing and Active Learning
Wenjun Qiu, David Lie, and Lisa Austin, University of Toronto

PolicyComp: Counterpart Comparison of Privacy Policies Uncovers Overbroad Personal Data
Collection Practices
Lu Zhou, Xidian University and Shanghai Jiao Tong University; Chengyongxiao Wei, Tong Zhu, and Guoxing Chen, Shanghai Jiao Tong University; Xiaokuan Zhang, George Mason University; Suguo Du, Hui Cao, and Haojin Zhu, Shanghai Jiao Tong University

Lalaine: Measuring and Characterizing Non-Compliance of Apple Privacy Labels
Yue Xiao, Zhengyi Li, and Yue Qin, Indiana University Bloomington; Xiaolong Bai, Orion Security Lab, Alibaba Group; Jiale Guan, Xiaojing Liao, and Luyi Xing, Indiana University Bloomington

Automated Cookie Notice Analysis and Enforcement
Rishabh Khandelwal and Asmit Nayak, University of Wisconsin—Madison; Hamza Harkous, Google, Inc.; Kassem Fawaz, University of Wisconsin—Madison

ML Applications to Malware
Continuous Learning for Android Malware Detection
Yizheng Chen, Zhoujie Ding, and David Wagner, UC Berkeley

Humans vs. Machines in Malware Classification
Simone Aonzo, EURECOM; Yufei Han, INRIA; Alessandro Mantovani and Davide Balzarotti, EURECOM

Adversarial Training for Raw-Binary Malware Classifiers
Keane Lucas, Samruddhi Pai, Weiran Lin, and Lujo Bauer, Carnegie Mellon University; Michael K. Reiter, Duke University; Mahmood Sharif, Tel Aviv University
Black-box Adversarial Example Attack towards FCG Based Android Malware Detection under Incomplete Feature Information

Heng Li, Huazhong University of Science and Technology; Zhang Cheng, NSFOCUS Technologies Group Co., Ltd. and Huazhong University of Science and Technology; Bang Wu, Liheng Yuan, Cuiying Gao, and Wei Yuan, Huazhong University of Science and Technology; Xiapu Luo, The Hong Kong Polytechnic University

Evading Provenance-Based ML Detectors with Adversarial System Actions

Kunal Mukherjee, Joshua Wiedemeier, Tianhao Wang, James Wei, Feng Chen, Muhyun Kim, Murat Kantarcioglu, and Kangkook Jee, The University of Texas at Dallas

Secure Messaging

TreeSync: Authenticated Group Management for Messaging Layer Security

Théophile Wallez, Inria Paris; Jonathan Protzenko, Microsoft Research; Benjamin Beurdouche, Mozilla; Karthikeyan Bhargavan, Inria Paris

Formal Analysis of Session-Handling in Secure Messaging: Lifting Security from Sessions to Conversations

Cas Cremers, CISPA Helmholtz Center for Information Security; Charlie Jacomme, Inria Paris; Aurora Naska, CISPA Helmholtz Center for Information Security

Cryptographic Administration for Secure Group Messaging

David Balbás, IMDEA Software Institute & Universidad Politécnica de Madrid; Daniel Collins and Serge Vaudenay, EPFL

Wink: Deniable Secure Messaging

Anrin Chakraborti, Duke University; Darius Suciu and Radu Sion, Stony Brook University

Three Lessons From Threema: Analysis of a Secure Messenger

Kenneth G. Paterson, Matteo Scarlata, and Kien Tuong Truong, ETH Zurich

x-Fuzz

MorFuzz: Fuzzing Processor via Runtime Instruction Morphing enhanced Synchronizable Co-simulation

Jinyan Xu and Yiyuan Liu, Zhejiang University; Sirui He, City University of Hong Kong; Haoran Lin and Yajin Zhou, Zhejiang University; Cong Wang, City University of Hong Kong

μFUZZ: Redesign of Parallel Fuzzing using Microservice Architecture

Yongheng Chen, Georgia Institute of Technology; Rui Zhong, Pennsylvania State University; Yupeng Yang, Georgia Institute of Technology; Hong Hu and Dinghao Wu, Pennsylvania State University; Wenke Lee, Georgia Institute of Technology

FishFuzz: Catch Deeper Bugs by Throwing Larger Nets

Han Zheng, National Computer Network Intrusion Protection Center, University of Chinese Academy of Science; School of Computer and Communication Sciences, EPFL; Zhongguancun Laboratory; Jiayuan Zhang, National Computer Network Intrusion Protection Center, University of Chinese Academy of Science; School of Computer and Communication, Lanzhou University of Technology; Yuhang Huang, National Computer Network Intrusion Protection Center, University of Chinese Academy of Science; Zezhong Ren, National Computer Network Intrusion Protection Center, University of Chinese Academy of Science; Zhongguancun Laboratory; He Wang, School of Cyber Engineering, Xidian University; Chunjie Cao, School of Cyberspace Security, Hainan University; Yuqing Zhang, National Computer Network Intrusion Protection Center, University of Chinese Academy of Science; Zhongguancun Laboratory; School of Cyberspace Security, Hainan University; School of Cyber Engineering, Xidian University; Flavio Toffalini and Mathias Payer, School of Computer and Communication Sciences, EPFL

HyPFuzz: Formal-Assisted Processor Fuzzing

Chen Chen, Rahul Kande, Nathan Nguyen, Flemming Andersen, and Aakash Tyagi, Texas A&M University; Ahmad-Reza Sadeghi, Technische Universität Darmstadt; Jayavijayan Rajendran, Texas A&M University

PolyFuzz: Holistic Greybox Fuzzing of Multi-Language Systems

Wen Li, Jinyang Ruan, and Guangbei Yi, Washington State University; Long Cheng, Clemson University; Xiapu Luo, The Hong Kong Polytechnic University; Haipeng Cai, Washington State University
Programs, Code, and Binaries

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

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

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

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

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

IoT Security Expectations and Barriers

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

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

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

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

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

Differential Privacy

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

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

What Are the Chances? Explaining the Epsilon Parameter in Differential Privacy ..................... 1613
Priyanka Nanayakkara, Northwestern University; Mary Anne Smart, University of California San Diego; Rachel Cummings, Columbia University; Gabriel Kapchuk, Boston University; Elissa M. Redmiles, Max Planck Institute for Software Systems
autofz: Automated Fuzzer Composition at Runtime ........................................ 1901
Yu-Fu Fu, Jaehyuk Lee, and Taesoo Kim, Georgia Institute of Technology

CarpetFuzz: Automatic Program Option Constraint Extraction from Documentation for Fuzzing ........ 1919
Dawei Wang, Ying Li, and Zhiyu Zhang, SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China; Kai Chen, SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China; Beijing Academy of Artificial Intelligence, China

Cache Attacks

SCARF – A Low-Latency Block Cipher for Secure Cache-Randomization .......................... 1937
Federico Canale, Ruhr-University Bochum; Tim Güneysu, Ruhr-University Bochum and DFKI; Gregor Leander and Jan Philipp Thoma, Ruhr-University Bochum; Yosuke Todo, NTT Social Informatics Laboratories; Rei Ueno, Tohoku University

The Gates of Time: Improving Cache Attacks with Transient Execution .......................... 1955
Daniel Katzman, Tel Aviv University; William Kosash, The University of Adelaide; Chitchanok Chuengsatiansup, The University of Melbourne; Eyal Ronen, Tel Aviv University; Yuval Yarom, The University of Adelaide

Synchronization Storage Channels (S²C): Timer-less Cache Side-Channel Attacks on the Apple M1 via Hardware Synchronization Instructions .......................................................... 1973
Jiyong Yu and Aishani Dutta, University of Illinois Urbana-Champaign; Trent Jaeger, Pennsylvania State University; David Kohlbrenner, University of Washington; Christopher W. Fletcher, University of Illinois Urbana-Champaign

CLEPSYDRACACHE – Preventing Cache Attacks with Time-Based Evictions ....................... 1991
Jan Philipp Thoma, Ruhr University Bochum; Christian Niesler, University of Duisburg-Essen; Dominic Funke, Gregor Leander, Pierre Mayr, and Nils Pohl, Ruhr University Bochum; Lucas Davi, University of Duisburg-Essen; Tim Güneysu, Ruhr University Bochum & DFKI

CACHESQL: Quantifying and Localizing Cache Side-Channel Vulnerabilities in Production Software ........ 2009
Yuanyuan Yuan, Zhibo Liu, and Shuai Wang, The Hong Kong University of Science and Technology

Authentication

InfinityGauntlet: Expose Smartphone Fingerprint Authentication to Brute-force Attack ............... 2027
Yu Chen and Yang Yu, Xuanwu Lab, Tencent; Lidong Zhai, Institute of Information Engineering, Chinese Academy of Sciences

A Study of Multi-Factor and Risk-Based Authentication Availability ..................................... 2043
Anthony Gavazzi, Ryan Williams, Engin Kirda, and Long Lu, Northeastern University; Andre King, Andy Davis, and Tim Leek, MIT Lincoln Laboratory

A Large-Scale Measurement of Website Login Policies ...................................................... 2061
Suood Al Roomi, Georgia Institute of Technology, Kuwait University; Frank Li, Georgia Institute of Technology

Security and Privacy Failures in Popular 2FA Apps ............................................................. 2079
Conor Gilsenan, UC Berkeley / ICSI; Fuzail Shakir and Noura Alomar, UC Berkeley; Serge Egelman, UC Berkeley / ICSI

Multi-Factor Key Derivation Function (MFKDF) for Fast, Flexible, Secure, & Practical Key Management .... 2097
Vivek Nair and Dawn Song, University of California, Berkeley

Private Data Leaks

Log: It's Big, It's Heavy, It’s Filled with Personal Data! Measuring the Logging of Sensitive Information in the Android Ecosystem ................................................................. 2115
Allan Lyons, University of Calgary; Julien Gamba, IMDEA Networks Institute and Universidad Carlos III de Madrid; Austin Shawaga, University of Calgary; Joel Reardon, University of Calgary and AppCensus, Inc.; Juan Tapiador, Universidad Carlos III de Madrid; Serge Egelman, ICSI and UC Berkeley and AppCensus, Inc.; Narseo Vallina-Rodriguez, IMDEA Networks Institute and AppCensus, Inc.

CodexLeaks: Privacy Leaks from Code Generation Language Models in GitHub Copilot .............. 2133
Liang Niu and Shujaat Mirza, New York University; Zayd Maradni and Christina Pöpper, New York University Abu Dhabi
Freaky Leaky SMS: Extracting User Locations by Analyzing SMS Timings .................................................. 2151
Evangelos Bitsikas, Northeastern University; Theodor Schnitzler, Research Center Trustworthy Data Science and Security; Christina Pöpper, New York University Abu Dhabi; Aanjhan Ranganathan, Northeastern University

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

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

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

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

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

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

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

Kailani R. Jones and Dalton A. Brucker-Hahn, University of Kansas; Bradley Fidler, Independent Researcher; Alexandru G. Bardas, University of Kansas

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

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

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

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

IvySyn: Automated Vulnerability Discovery in Deep Learning Frameworks .............................................. 2383
Neophytos Christou, Di Jin, and Vaggelis Atlidakis, Brown University; Baishakhi Ray, Columbia University; Vasileios P. Kemerlis, Brown University
Thursday, August 10

Smart? Assistants

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

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

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

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

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

Security-Adjacent Worker Perspectives

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

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

Alexander Krause, CISPA Helmholtz Center for Information Security; Jan H. Klemmer and Nicolas Huaman, Leibniz University Hannover; Dominik Wermke, CISPA Helmholtz Center for Information Security; Yasemin Acar, Paderborn University, George Washington University; Sascha Fahl, CISPA Helmholtz Center for Information Security

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

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

Censorship and Internet Freedom

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

A Study of China’s Censorship and Its Evasion Through the Lens of Online Gaming ........................................ 2599
Yuzhou Feng, Florida International University; Ruyu Zhai, Hangzhou Dianzi University; Radu Sion, Stony Brook University; Bogdan Carbunar, Florida International University
DeResistor: Toward Detection-Resistant Probing for Evasion of Internet Censorship ........................................ 2617
Abderrahmen Amich and Birhanu Eshete, University of Michigan, Dearborn; Vinod Yegneswaran, SRI International;
Nguyen Phong Hoang, University of Chicago

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

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

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

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

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

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

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

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

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

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

XCheck: Verifying Integrity of 3D Printed Patient-Specific Devices via Computing Tomography .................. 2815
Zhiyuan Yu, Yuanhaur Chang, Shixuan Zhai, Nicholas Deily, and Tao Ju, Washington University in St. Louis;
XiaoFeng Wang, Indiana University Bloomington; Uday Jammalamadaka, Rice University; Ning Zhang,
Washington University in St. Louis
Inducing Authentication Failures to Bypass Credit Card PINs
David Basin, Patrick Schaller, and Jorge Toro-Pozo, ETH Zurich

An Empirical Study & Evaluation of Modern CAPTCHAs
Andrew Searles, University of California, Irvine; Yoshimichi Nakatsuka, ETH Zurich; Ercan Ozturk, University of California, Irvine; Andrew Paverd, Microsoft; Gene Tsudik, University of California, Irvine; Ai Enkoji, Lawrence Livermore National Laboratory

Account Verification on Social Media: User Perceptions and Paid Enrollment
Madelyne Xiao, Mona Wang, Anunay Kulshrestha, and Jonathan Mayer, Princeton University

DNS Security
User Awareness and Behaviors Concerning Encrypted DNS Settings in Web Browsers
Alexandra Nisenoff, Carnegie Mellon University and University of Chicago; Ranya Sharma and Nick Feamster, University of Chicago

Two Sides of the Shield: Understanding Protective DNS adoption factors
Elsa Rodriguez, Radu Anghel, Simon Parkin, Michel van Eeten, and Carlos Gañán, Delft University of Technology

The Maginot Line: Attacking the Boundary of DNS Caching Protection
Xiang Li, Chaoyi Lu, and Baojun Liu, Tsinghua University; Qifan Zhang and Zhou Li, University of California, Irvine; Haixin Duan, Tsinghua University, QI-ANXIN Technology Research Institute, and Zhongguancun Laboratory; Qi Li, Tsinghua University and Zhongguancun Laboratory

Fourteen Years in the Life: A Root Server’s Perspective on DNS Resolver Security
Alden Hilton, Sandia National Laboratories; Casey Deccio, Brigham Young University; Jacob Davis, Sandia National Laboratories

NRDelegationAttack: Complexity DDoS attack on DNS Recursive Resolvers
Yehuda Afek and Anat Bremler-Barr, Tel-Aviv University; Shani Stajnrod, Reichman University

Graphs and Security
Inductive Graph Unlearning
Cheng-Long Wang, King Abdullah University of Science and Technology and SDAIA-KAUST Center of Excellence in Data Science and Artificial Intelligence; Mengdi Huai, Iowa State University; Di Wang, King Abdullah University of Science and Technology, Computational Bioscience Research Center, and SDAIA-KAUST Center of Excellence in Data Science and Artificial Intelligence

GAP: Differentially Private Graph Neural Networks with Aggregation Perturbation
Sina Sajadmanesh, Idiap Research Institute and EPFL; Ali Shahin Shamsabadi, Alan Turing Institute; Aurélien Bellet, Inria; Daniel Gatica-Perez, Idiap Research Institute and EPFL

PrivGraph: Differentially Private Graph Data Publication by Exploiting Community Information
Quan Yuan, Zhejiang University; Zhikun Zhang, Stanford University and CISPA Helmholtz Center for Information Security; Linkang Du, Zhejiang University; Min Chen, CISPA Helmholtz Center for Information Security; Peng Cheng and Mingyang Sun, Zhejiang University

On the Security Risks of Knowledge Graph Reasoning
Zhaohan Xi, Tianyu Du, Changjiang Li, and Ren Pang, Pennsylvania State University; Shouling Ji, Zhejiang University; Xiapu Luo, The Hong Kong Polytechnic University; Xusheng Xiao, Arizona State University; Fenglong Ma and Ting Wang, Pennsylvania State University

The Case for Learned Provenance Graph Storage Systems
Hailun Ding, Juan Zhai, Dong Deng, and Shiqing Ma, Rutgers University

Ethereum Security
A Large Scale Study of the Ethereum Arbitrage Ecosystem
Robert McLaughlin, Christopher Kruegel, and Giovanni Vigna, University of California, Santa Barbara

ACon²: Adaptive Conformal Consensus for Provable Blockchain Oracles
Sangdon Park, Georgia Institute of Technology; Osbert Bastani, University of Pennsylvania; Taesoo Kim, Georgia Institute of Technology
Snapping Snap Sync: Practical Attacks on Go Ethereum Synchronising Nodes ................................. 3331
Massimiliano Taverna and Kenneth G. Paterson, ETH Zurich

Token Spammers, Rug Pulls, and Sniper Bots: An Analysis of the Ecosystem of Tokens in Ethereum and in the Binance Smart Chain (BNB) .......................................................... 3349
Federico Cernera, Massimo La Morgia, Alessandro Mei, and Francesco Sassi, Sapienza University of Rome

Automated Inference on Financial Security of Ethereum Smart Contracts ........................................ 3367
Wansen Wang and Wenchao Huang, University of Science and Technology of China; Zhaoyi Meng, Anhui University; Yan Xiong and Fuyou Miao, University of Science and Technology of China; Xianjin Fang, Anhui University of Science and Technology; Caichang Tu and Renjie Ji, University of Science and Technology of China

Supply Chains and Third-Party Code

LibScan: Towards More Precise Third-Party Library Identification for Android Applications .................. 3385
Yafei Wu and Cong Sun, State Key Lab of ISN, School of Cyber Engineering, Xidian University, China; Dongrui Zeng, Palo Alto Networks, Inc., Santa Clara, CA, USA; Gang Tan, The Pennsylvania State University, University Park, PA, USA; Siqi Ma, University of New South Wales, Australia; Peicheng Wang, State Key Lab of ISN, School of Cyber Engineering, Xidian University, China

Union under Duress: Understanding Hazards of Duplicate Resource Mismediation in Android Software Supply Chain ................................................................. 3403
Xueqiang Wang, University of Central Florida; Yifan Zhang and Xiaofeng Wang, Indiana University Bloomington; Yan Jia, Nankai University; Luyi Xing, Indiana University Bloomington

UVMScan: Detecting Third-Party Component Usage Violations in IoT Firmware .............................. 3421
Binbin Zhao, Georgia Institute of Technology and Zhejiang University; Shouling Ji and Xuhong Zhang, Zhejiang University; Yuan Tian, University of California, Los Angeles; Qinying Wang, Yuwen Pu, and Chenyang Lyu, Zhejiang University; Raheem Beyah, Georgia Institute of Technology

Beyond Typosquatting: An In-depth Look at Package Confusion .................................................. 3439
Shradha Neupane, Worcester Polytechnic Institute; Grant Holmes, Elizabeth Wyss, and Drew Davidson, University of Kansas; Lorenzo De Carli, University of Calgary

SANDDriller: A Fully-Automated Approach for Testing Language-Based JavaScript Sandboxes .............. 3457
Abdullah AlHamdan and Cristian-Alexandru Staicu, CISPA Helmholtz Center for Information Security

Cellular Networks

Instructions Unclear: Undefined Behaviour in Cellular Network Specifications ............................... 3475
Daniel Klischies, Ruhr University Bochum; Moritz Schloegel and Tobias Scharnowski, CISPA Helmholtz Center for Information Security; Mikhail Bogodukhov, Independent; David Rupprecht, Radix Security; Veelasha Moonsamy, Ruhr University Bochum

MOBILEATLAS: Geographically Decoupled Measurements in Cellular Networks for Security and Privacy Research .......................... 3493
Gabriel K. Gegenhuber, University of Vienna; Wilfried Mayer, SBA Research; Edgar Weippl, University of Vienna; Adrian Dabrowski, CISPA Helmholtz Center for Information Security

Eavesdropping Mobile App Activity via Radio-Frequency Energy Harvesting ................................ 3511
Tao Ni, Shenzhen Research Institute, City University of Hong Kong, and Department of Computer Science, City University of Hong Kong; Guohao Lan, Department of Software Technology, Delft University of Technology; Jia Wang, College of Computer Science and Software Engineering, Shenzhen University; Qingchuan Zhao, Department of Computer Science, City University of Hong Kong; Weitao Xu, Shenzhen Research Institute, City University of Hong Kong, and Department of Computer Science, City University of Hong Kong

Sherlock on Specs: Building LTE Conformance Tests through Automated Reasoning ....................... 3529
Yi Chen and Di Tang, Indiana University Bloomington; Yepeng Yao, {CAS-KLONAT, BKLONSPT}, Institute of Information Engineering, CAS, and School of Cyber Security, University of Chinese Academy of Sciences; Mingming Zha and Xiaofeng Wang, Indiana University Bloomington; Xiaozhong Liu, Worcester Polytechnic Institute; Haixu Tang, Indiana University Bloomington; Baoxu Liu, {CAS-KLONAT, BKLONSPT}, Institute of Information Engineering, CAS, and School of Cyber Security, University of Chinese Academy of Sciences
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BaseComp: A Comparative Analysis for Integrity Protection in Cellular Baseband Software</strong></td>
<td>3547</td>
</tr>
<tr>
<td>Eunsoo Kim, Min Woo Baek, and CheolJun Park, KAIST; Dongkwan Kim, Samsung SDS; Yongdae Kim and</td>
<td></td>
</tr>
<tr>
<td>Insu Yun, KAIST</td>
<td></td>
</tr>
<tr>
<td><strong>Usability and User Perspectives</strong></td>
<td>3565</td>
</tr>
<tr>
<td>Investigating Verification Behavior and Perceptions of Visual Digital Certificates</td>
<td></td>
</tr>
<tr>
<td>Dafniel Gerhardt and Alexander Ponticello, CISPA Helmholtz Center for Information Security and</td>
<td></td>
</tr>
<tr>
<td>Saarland University; Adrian Dabrowski and Katharina Krombholz, CISPA Helmholtz Center for</td>
<td></td>
</tr>
<tr>
<td>Information Security</td>
<td></td>
</tr>
<tr>
<td>“My Privacy for their Security”: Employees’ Privacy Perspectives and Expectations when using</td>
<td></td>
</tr>
<tr>
<td>Enterprise Security Software</td>
<td></td>
</tr>
<tr>
<td>Jonah Stegman, Patrick J. Trottier, Caroline Hillier, and Hassan Khan, University of Guelph;</td>
<td></td>
</tr>
<tr>
<td>Mohammad Mannan, Concordia University</td>
<td></td>
</tr>
<tr>
<td><strong>Account Security Interfaces: Important, Unintuitive, and Untrustworthy.</strong></td>
<td>3601</td>
</tr>
<tr>
<td>Alaa Daffalla and Marina Bohuk, Cornell University; Nicola Dell, Jacobs Institute Cornell Tech;</td>
<td></td>
</tr>
<tr>
<td>Rosanna Bellini, Cornell University; Thomas Ristenpart, Cornell Tech</td>
<td></td>
</tr>
<tr>
<td>Defining “Broken”: User Experiences and Remediation Tactics When Ad-Blocking or Tracking-Protection Tools Break a Website’s User Experience</td>
<td></td>
</tr>
<tr>
<td>Alexandra Nisenoff, University of Chicago and Carnegie Mellon University; Arthur Borem, Madison</td>
<td></td>
</tr>
<tr>
<td>Pickering, Grant Nakanishi, Maya Thumpasery, and Blase Ur, University of Chicago</td>
<td></td>
</tr>
<tr>
<td><strong>Cryptographic Deniability: A Multi-perspective Study of User Perceptions and Expectations</strong></td>
<td>3637</td>
</tr>
<tr>
<td>Tarun Kumar Yadav, Brigham Young University; Devashish Gosain, KU Leuven; Kent Seamons, Brigham</td>
<td></td>
</tr>
<tr>
<td>Young University</td>
<td></td>
</tr>
<tr>
<td><strong>Entomology</strong></td>
<td>3655</td>
</tr>
<tr>
<td>Silent Bugs Matter: A Study of Compiler-Introduced Security Bugs</td>
<td></td>
</tr>
<tr>
<td>Jianhao Xu, Nanjing University; Kangjie Lu, University of Minnesota; Zhengjie Du, Zhu Ding, and</td>
<td></td>
</tr>
<tr>
<td>Linke Li, Nanjing University; Qiushi Wu, University of Minnesota; Mathias Payer, EPFL; Bing</td>
<td></td>
</tr>
<tr>
<td>Mao, Nanjing University</td>
<td></td>
</tr>
<tr>
<td>A Bug’s Life: Analyzing the Lifecycle and Mitigation Process of Content Security Policy Bugs</td>
<td>3673</td>
</tr>
<tr>
<td>Gertjan Franken, Tom Van Goethem, Lieven Desmet, and Wouter Joosen, imec-DistriNet, KU Leuven</td>
<td></td>
</tr>
<tr>
<td><strong>Remote Code Execution from SSTI in the Sandbox: Automatically Detecting and Exploiting Template</strong></td>
<td></td>
</tr>
<tr>
<td>Yudi Zhao, Yuan Zhang, and Min Yang, Fudan University</td>
<td>3691</td>
</tr>
<tr>
<td><strong>Detecting API Post-Handling Bugs Using Code and Description in Patches</strong></td>
<td>3709</td>
</tr>
<tr>
<td>Miaoqian Lin, Kai Chen, and Yang Xiao, Institute of Information Engineering, Chinese Academy</td>
<td></td>
</tr>
<tr>
<td>of Sciences, China; School of Cyber Security, University of Chinese Academy of Sciences, China</td>
<td></td>
</tr>
<tr>
<td>Place Your Locks Well: Understanding and Detecting Lock Misuse Bugs</td>
<td>3727</td>
</tr>
<tr>
<td>Yuandao Cai, Peisen Yao, Chengfeng Ye, and Charles Zhang, The Hong Kong University of Science and</td>
<td></td>
</tr>
<tr>
<td>Technology</td>
<td></td>
</tr>
<tr>
<td><strong>Adversarial Examples</strong></td>
<td>3745</td>
</tr>
<tr>
<td>The Space of Adversarial Strategies</td>
<td></td>
</tr>
<tr>
<td>Ryan Sheatsley, Blaine Hoak, Eric Pauley, and Patrick McDaniel, University of Wisconsin-Madison</td>
<td></td>
</tr>
<tr>
<td>“Security is not my field, I’m a stats guy”: A Qualitative Root Cause Analysis of Barriers to</td>
<td></td>
</tr>
<tr>
<td>Adversarial Machine</td>
<td>3763</td>
</tr>
<tr>
<td>Learning Defenses in Industry</td>
<td></td>
</tr>
<tr>
<td>Jaron Mink, University of Illinois at Urbana-Champaign; Harjot Kaur, Leibniz University</td>
<td></td>
</tr>
<tr>
<td>Hannover; Juliane Schmüser and Sascha Fahl, CISPA Helmholtz Center for Information Security;</td>
<td></td>
</tr>
<tr>
<td>Yasemin Acar, Paderborn University and George Washington University</td>
<td></td>
</tr>
<tr>
<td><strong>X-Adv: Physical Adversarial Object Attacks against X-ray Prohibited Item Detection</strong></td>
<td>3781</td>
</tr>
<tr>
<td>Aishan Liu and Jun Guo, Beihang University; Jiajai Wang, Zhongguancun Laboratory; Siyuan Liang,</td>
<td></td>
</tr>
<tr>
<td>Chinese Academy of Sciences; Renshuai Tao, Beihang University; Wenbo Zhou, University of Science</td>
<td></td>
</tr>
<tr>
<td>and Technology of China; Cong Liu, iFLYTEK; Xianglong Liu, Beihang University, Zhongguancun</td>
<td></td>
</tr>
<tr>
<td>Laboratory, and Hefei Comprehensive National Science Center; Dacheng Tao, JD Explore Academy</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>SMACK: Semantically Meaningful Adversarial Audio Attack</td>
<td>3799</td>
</tr>
<tr>
<td>Zhiyuan Yu, Yuanhaur Chang, and Ning Zhang, Washington University in St. Louis; Chaowei Xiao, Arizona State University</td>
<td></td>
</tr>
<tr>
<td>URET: Universal Robustness Evaluation Toolkit (for Evasion)</td>
<td>3817</td>
</tr>
<tr>
<td>Kevin Eykholt, Taesung Lee, Douglas Schales, Jiyong Jang, and Ian Molloy, IBM Research; Masha Zorin, University of Cambridge</td>
<td></td>
</tr>
<tr>
<td>Private Record Access</td>
<td>3835</td>
</tr>
<tr>
<td>Authenticated private information retrieval</td>
<td></td>
</tr>
<tr>
<td>Simone Colombo, EPFL; Kirill Nikitin, Cornell Tech; Henry Corrigan-Gibbs, MIT; David J. Wu, UT Austin; Bryan Ford, EPFL</td>
<td></td>
</tr>
<tr>
<td>Don’t be Dense: Efficient Keyword PIR for Sparse Databases</td>
<td>3853</td>
</tr>
<tr>
<td>Sarvar Patel and Joon Young Seo, Google; Kevin Yeo, Google and Columbia University</td>
<td></td>
</tr>
<tr>
<td>GigaDORAM: Breaking the Billion Address Barrier</td>
<td>3871</td>
</tr>
<tr>
<td>Brett Falk, University of Pennsylvania; Rafail Ostrovsky, Matan Shtepel, and Jacob Zhang, University of California, Los Angeles</td>
<td></td>
</tr>
<tr>
<td>Alexandra Henzinger, Matthew M. Hong, and Henry Corrigan-Gibbs, MIT; Sarah Meiklejohn, Google; Vinod Vaikuntanathan, MIT</td>
<td></td>
</tr>
<tr>
<td>DuORAM: A Bandwidth-Efficient Distributed ORAM for 2- and 3-Party Computation</td>
<td>3907</td>
</tr>
<tr>
<td>Adithya Vadapalli, University of Waterloo; Ryan Henry, University of Calgary; Ian Goldberg, University of Waterloo</td>
<td></td>
</tr>
<tr>
<td>It’s All Fun and Games Until...</td>
<td>3925</td>
</tr>
<tr>
<td>A Peek into the Metaverse: Detecting 3D Model Clones in Mobile Games</td>
<td></td>
</tr>
<tr>
<td>Chaoshun Zuo, Chao Wang, and Zhiqiang Lin, The Ohio State University</td>
<td></td>
</tr>
<tr>
<td>PATROL: Provable Defense against Adversarial Policy in Two-player Games</td>
<td>3943</td>
</tr>
<tr>
<td>Wenbo Guo, UC Berkeley; Xian Wu, Northwestern University; Lun Wang, UC Berkeley; Xinyu Xing, Northwestern University; Dawn Song, UC Berkeley</td>
<td></td>
</tr>
<tr>
<td>The Blockchain Imitation Game</td>
<td>3961</td>
</tr>
<tr>
<td>Kaihua Qin, Imperial College London, RDI; Stefanos Chaliasos, Imperial College London; Liyi Zhou, Imperial College London, RDI; Benjamin Livshits, Imperial College London; Dawn Song, UC Berkeley, RDI; Arthur Gervais, University College London, RDI</td>
<td></td>
</tr>
<tr>
<td>It’s all in your head(set): Side-channel attacks on AR/VR systems</td>
<td>3979</td>
</tr>
<tr>
<td>Yicheng Zhang, Carter Slocum, Jiasi Chen, and Nael Abu-Ghazaleh, University of California, Riverside</td>
<td></td>
</tr>
<tr>
<td>Egg Hunt in Tesla Infotainment: A First Look at Reverse Engineering of Qt Binaries</td>
<td>3997</td>
</tr>
<tr>
<td>Haohuang Wen and Zhiqiang Lin, The Ohio State University</td>
<td></td>
</tr>
<tr>
<td>Enclaves and Serverless Computing</td>
<td>4015</td>
</tr>
<tr>
<td>Reusable Enclaves for Confidential Serverless Computing</td>
<td></td>
</tr>
<tr>
<td>Shixuan Zhao, The Ohio State University; Pinshen Xu, Southern University of Science and Technology; Guoxing Chen, Shanghai Jiao Tong University; Mengya Zhang, The Ohio State University; Yinqian Zhang, Southern University of Science and Technology; Zhiqiang Lin, The Ohio State University</td>
<td></td>
</tr>
<tr>
<td>enigmAp: External-Memory Oblivious Map for Secure Enclaves</td>
<td>4033</td>
</tr>
<tr>
<td>Afonso Tinoco, Sixiang Gao, and Elaine Shi, CMU</td>
<td></td>
</tr>
<tr>
<td>AEX-Notify: Thwarting Precise Single-Stepping Attacks through Interrupt Awareness for Intel SGX Enclaves</td>
<td>4051</td>
</tr>
<tr>
<td>Scott Constable, Intel Corporation; Jo Van Bulck, imec-DistriNet, KU Leuven; Xiang Cheng, Georgia Institute of Technology; Yuan Xiao, Cedric Xing, and Ilya Alexandrovich, Intel Corporation; Taesoo Kim, Georgia Institute of Technology; Frank Piessens, imec-DistriNet, KU Leuven; Mona Vij, Intel Corporation; Mark Silberstein, Technion</td>
<td></td>
</tr>
<tr>
<td>Controlled Data Races in Enclaves: Attacks and Detection</td>
<td>4069</td>
</tr>
<tr>
<td>Sanchuan Chen, Fordham University; Zhiqiang Lin, The Ohio State University; Yinqian Zhang, Southern University of Science and Technology</td>
<td></td>
</tr>
</tbody>
</table>
Guarding Serverless Applications with Kalium ........................................... 4087
Deepak Sirone Jegan, University of Wisconsin-Madison; Liang Wang, Princeton University; Siddhant Bhagat, Microsoft;
Michael Swift, University of Wisconsin-Madison

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

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

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

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

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

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

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

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

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

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

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

ARGUS: Context-Based Detection of Stealthy IoT Infiltration Attacks ............................... 4301
Phillip Rieger, Marco Chiese, Reham Mohamed, Markus Miettinen, Hossein Fereidooni, and Ahmad-Reza Sadeghi, Technical University of Darmstadt
Generative Intrusion Detection and Prevention on Data Stream .......................... 4319
HyungBin Seo and MyungKeun Yoon, Kookmin University

xNIDS: Explaining Deep Learning-based Network Intrusion Detection Systems for Active Intrusion Responses .......................... 4337
Feng Wei, University at Buffalo; Hongda Li, Palo Alto Networks; Ziming Zhao and Hongxin Hu, University at Buffalo

ProGRapher: An Anomaly Detection System based on Provenance Graph Embedding ........................................ 4355
Fan Yang, The Chinese University of Hong Kong; Jiacen Xu, University of California, Irvine; Chunlin Xiong, Sangfor Technologies Inc.; Zhou Li, University of California, Irvine; Kehuan Zhang, The Chinese University of Hong Kong

Privacy Preserving Crypto Blocks

Dubhe: Zero-Knowledge Proofs for Standard AES and related Applications .................. 4373
Changchang Ding and Yan Huang, Indiana University Bloomington

Curv Trees: Practical and Transparent Zero-Knowledge Accumulators .......................... 4391
Matteo Campanelli, Protocol Labs; Mathias Hall-Andersen and Simon Holmegaard Kamp, Aarhus University, Denmark

BalanceProoF: Maintainable Vector Commitments with Fast Aggregation .................. 4409
Weijie Wang, Annie Ulichney, and Charalampos Papamanthou, Yale University

zkSaaS: Zero-Knowledge SNARKs as a Service .................................................. 4427
Sanjam Garg, University of California, Berkeley, and NTT Research; Aarushi Goel, NTT Research; Abhishek Jain, Johns Hopkins University; Guru-Vamsi Policharla and Sruthi Sekar, University of California, Berkeley

VeriZene: Decentralized Private Computation with Universal Setup .......................... 4445
Alex Luoyuan Xiong, Espresso Systems, National University of Singapore; Binyi Chen and Zhenfei Zhang, Espresso Systems; Benedikt Bünz, Espresso Systems, Stanford University; Ben Fisch, Espresso Systems, Yale University; Fernando Krell and Philippe Camacho, Espresso Systems

Warm and Fuzzing

INTENDER: Fuzzing Intent-Based Networking with Intent-State Transition Guidance .................. 4463
Jiwon Kim, Purdue University; Benjamin E. Ujcich, Georgetown University; Dave (Jing) Tian, Purdue University

BLEEM: Packet Sequence Oriented Fuzzing for Protocol Implementations .................. 4481
Zhengxiong Luo, Junze Yu, Feilong Zuo, Jianzhong Liu, and Yu Jiang, Tsinghua University; Ting Chen, University of Electronic Science and Technology of China; Abhik Roychoudhury, National University of Singapore; Jiaguang Sun, Tsinghua University

Automated Exploitable Heap Layout Generation for Heap Overflows Through Manipulation .................................................. 4499
Bin Zhang, Jiongyi Chen, Runhaor Li, Chao Feng, Ruilin Li, and Chaojing Tang, National University of Defense Technology

Distance-Guided Fuzzing .................................................. 4517
Chenyang Lyu, Jiacheng Xu, Shouling Ji, Xuhong Zhang, and Qinyying Wang, Zhejiang University; Binbin Zhao, Georgia Institute of Technology; Gaoning Pan, Zhejiang University; Wei Cao and Peng Chen, Ant Group; Raheem Beyah, Georgia Institute of Technology

Systematic Assessment of Fuzzers using Mutation Analysis ........................................ 4535
Philipp Görz, Björn Mathis, and Keno Hassler, CISPA Helmholtz Center for Information Security; Emre Güler, Ruhr-Universität Bochum; Thorsten Holz and Andreas Zeller, CISPA Helmholtz Center for Information Security; Rahul Gopinath, University of Sydney

Remote Attacks

HomeSpy: The Invisible Sniffer of Infrared Remote Control of Smart TVs .................. 4553
Kong Huang, YuTong Zhou, and Ke Zhang, The Chinese University of Hong Kong; Jiacen Xu, University of California, Irvine; Jiongyi Chen, National University of Defense Technology; Di Tang, Indiana University Bloomington; Kehuan Zhang, The Chinese University of Hong Kong
Network Cryptographic Protocols

Keep Your Friends Close, but Your Routeservers Closer: Insights into RPKI Validation in the Internet ........ 4841
Tomas Hlavacek, Fraunhofer Institute for Secure Information Technology SIT and National Research Center for Applied Cybersecurity ATHENE; Haya Shulman and Niklas Vogel, Fraunhofer Institute for Secure Information Technology SIT, National Research Center for Applied Cybersecurity ATHENE, and Goethe-Universität Frankfurt; Michael Waidner, Fraunhofer Institute for Secure Information Technology SIT, National Research Center for Applied Cybersecurity ATHENE, and Technische Universität Darmstadt

Exploring the Unknown DTLS Universe: Analysis of the DTLS Server Ecosystem on the Internet .......... 4859
Nurullah Erinola and Marcel Maehren, Ruhr University Bochum; Robert Merget, Technology Innovation Institute; Juraj Somorovsky, Paderborn University; Jörg Schwenk, Ruhr University Bochum

We Really Need to Talk About Session Tickets: A Large-Scale Analysis of Cryptographic Dangers with TLS Session Tickets ................................................................. 4877
Sven Hebrok, Paderborn University; Simon Nachtigall, Paderborn University and achelos GmbH; Marcel Maehren and Nurullah Erinola, Ruhr University Bochum; Robert Merget, Technology Innovation Institute and Ruhr University Bochum; Juraj Somorovsky, Paderborn University; Jörg Schwenk, Ruhr University Bochum

Extended Hello(): A Comprehensive Large-Scale Study on Email Confidentiality and Integrity Mechanisms in the Wild ................................................................. 4895
Birk Blechschmidt, Saarland University; Ben Stock, CISPA Helmholtz Center for Information Security

Warmer and Fuzzers

No Linux, No Problem: Fast and Correct Windows Binary Fuzzing via Target-embedded Snapshotting .... 4913
Leo Stone and Rishi Ranjan, Virginia Tech; Stefan Nagy, University of Utah; Matthew Hicks, Virginia Tech

DAFL: Directed Grey-box Fuzzing guided by Data Dependency .................................................... 4931
Tae Eun Kim, KAIST; Jaeseung Choi, Sogang University; Kihong Heo and Sang Kil Cha, KAIST

DynSQL: Stateful Fuzzing for Database Management Systems with Complex and Valid SQL Query Generation . . 4949
Zu-Ming Jiang, ETH Zurich; Jia-Ju Bai, Tsinghua University; Zhendong Su, ETH Zurich

AIFORE: Smart Fuzzing Based on Automatic Input Format Reverse Engineering .......................... 4967
Ji Shi, (CAS-KLONAT, BKLONSPT), Institute of Information Engineering, Chinese Academy of Sciences; Institute for Network Science and Cyberspace & BNRist, Tsinghua University; Zhongguancun Lab; Singular Security Lab, Huawei Technologies; School of Cyber Security, University of Chinese Academy of Sciences; Zhun Wang, Institute for Network Science and Cyberspace & BNRist, Tsinghua University; Zhongguancun Lab; Zhiyao Feng, Institute for Network Science and Cyberspace & BNRist, Tsinghua University; Zhongguancun Lab; EPFL; Yang Lan and Shisong Qin, Institute for Network Science and Cyberspace & BNRist, Tsinghua University; Zhongguancun Lab; Wei You, Renmin University of China; Wei Zou, (CAS-KLONAT, BKLONSPT), Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences; Mathias Payer, EPFL; Chao Zhang, Institute for Network Science and Cyberspace & BNRist, Tsinghua University; Zhongguancun Lab

Friday, August 11

Kernel Analysis

BoKASAN: Binary-only Kernel Address Sanitizer for Effective Kernel Fuzzing .............................. 4985
Mingi Cho, Dohyeon An, Hoyong Jin, and Taekyoung Kwon, Yonsei University

ACTor: Action-Guided Kernel Fuzzing ............................................................................................... 5003
Marius Fleischer, Dipanjan Das, and Priyanka Bose, University of California, Santa Barbara; Weiheng Bai and Kangjie Lu, University of Minnesota; Mathias Payer, EPFL; Christopher Kruegel and Giovanni Vigna, University of California, Santa Barbara

FirmSolo: Enabling dynamic analysis of binary Linux-based IoT kernel modules .......................... 5021
Ioannis Angelakopoulos, Gianluca Stringhini, and Manuel Egele, Boston University

KextFuzz: Fuzzing macOS Kernel EXTensions on Apple Silicon via Exploiting Mitigations .......... 5039
Tingting Yin, Tsinghua University and Ant Group; Zicong Gao, State Key Laboratory of Mathematical Engineering and Advanced Computing; Zhenghang Xiao, Hunan University; Zheyu Ma, Tsinghua University; Min Zheng, Ant Group; Chao Zhang, Tsinghua University and Zhongguancun Laboratory
unConTAined: Uncovering Container Confusion in the Linux Kernel ........................................ 5055
Jakob Koschel, Vrije Universiteit Amsterdam; Pietro Borrello and Daniele Cono D’Elia, Sapienza University of Rome; Herbert Bos and Cristiano Giuffrida, Vrije Universiteit Amsterdam

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

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

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

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

Tadayoshi Kohno, University of Washington; Yasemin Acar, Paderborn University & George Washington University; Wulf Loh, Universität Tübingen

De-anonymization and Re-identification
CATCH YOU AND I CAN: Revealing Source Voiceprint Against Voice Conversion ........................... 5163
Jiangyi Deng, Yanjiao Chen, Yinan Zhong, and Qianhao Miao, Zhejiang University; Xueluan Gong, Wuhan University; Wenyuan Xu, Zhejiang University

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

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

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

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

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

PCAT: Functionality and Data Stealing from Split Learning by Pseudo-Client Attack .......................... 5271
Xinben Gao and Lan Zhang, University of Science and Technology of China
A Plot is Worth a Thousand Words: Model Information Stealing Attacks via Scientific Plots  5289
Boyang Zhang and Xinlei He, CISPA Helmholtz Center for Information Security; Yun Shen, NetApp; Tianhao Wang, University of Virginia; Yang Zhang, CISPA Helmholtz Center for Information Security

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

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

Distributed Secure Computations

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

Practical Asynchronous High-threshold Distributed Key Generation and Distributed Polynomial Sampling  5359
Sourav Das, University of Illinois at Urbana-Champaign; Zhoulun Xiang, Apts; Letefers Kokoris-Kogias, IST Austria and Myster Labs; Ling Ren, University of Illinois at Urbana-Champaign

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

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

Mobile Security and Privacy

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

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

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

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

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

Web Security

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

Cookie Crumbles: Breaking and Fixing Web Session Integrity  5539
Marco Squarcina, TU Wien; Pedro Adão, Instituto Superior Técnico, ULisboa, Instituto de Telecomunicações; Lorenzo Veronese and Matteo Maffei, TU Wien
**FuncTeller: How Well Does eFPGA Hide Functionality?** .................................................. 5809
Zhaokun Han, Texas A&M University; Mohammed Shayan, The University of Texas at Dallas; Aneesh Dixit, Texas A&M University; Mustafa Shihab and Yiorgos Makris, The University of Texas at Dallas; Jeyavijayan (JV) Rajendran, Texas A&M University

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

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

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

**Attacks on Cryptography**

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

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

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

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

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

**Cloud Insecurity**

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

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

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

**Detecting Multi-Step IAM Attacks in AWS Environments via Model Checking** .......................... 6025
Ilia Shevrin, Citi; Oded Margalit, Ben-Gurion University
Remote Direct Memory Introspection .................................................. 6043
Hongyi Liu, Jiarong Xing, and Yibo Huang, Rice University; Danyang Zhuo, Duke University; Srinivas Devadas, Massachusetts Institute of Technology; Ang Chen, Rice University

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Secure Floating-Point Training ........................................... 6329
Deevashwer Rathee, University of California, Berkeley; Anwesh Bhattacharya, Divya Gupta, and Rahul Sharma, Microsoft Research; Dawn Song, University of California, Berkeley

NeuroPots: Realtime Proactive Defense against Bit-Flip Attacks in Neural Networks ............................................. 6347
Qi Liu, Lehigh University; Jieming Yin, Nanjing University of Posts and Telecommunications; Wujie Wen, Lehigh University; Chengmo Yang, University of Delaware; Shi Sha, Wilkes University

FedVal: Different good or different bad in federated learning ................................................................. 6365
Viktor Valadi, AI Sweden; Xinchui Qiu, Pedro Porto Buarque de Gusmão, and Nicholas D. Lane, University of Cambridge; Mina Alibeigi, University of Cambridge and Zenseact AB

Gradient Obfuscation Gives a False Sense of Security in Federated Learning .................................. 6381
Kai Yue, North Carolina State University; Richeng Jin, Zhejiang University; Chau-Wai Wong, Dror Baron, and Huaiyu Dai, North Carolina State University

Cryptography for Privacy

Prime Match: A Privacy-Preserving Inventory Matching System .................................................... 6417
Antigoni Polychroniadou, J.P. Morgan; Gilad Asharov, Bar-Ilan University; Benjamin Diamond, Tucker Balch, Hans Buehler, Richard Hua, Suwen Gu, Greg Gimler, and Manuela Veloso, J.P. Morgan

Squirrel: A Scalable Secure Two-Party Computation Framework for Training Gradient Boosting Decision Tree 6435
Wen-jie Lu and Zhichong Huang, Alibaba Group; Qizhi Zhang, Ant Group; Yuchen Wang, Alibaba Group; Cheng Hong, Ant Group

EOS: Efficient Private Delegation of zkSNARK Provers ................................................................. 6453
Alessandro Chiesa, UC Berkeley and EPFL; Ryan Lehmkuhl, MIT; Pratyush Mishra, Aleo and University of Pennsylvania; Yinuo Zhang, UC Berkeley

Machine-checking Multi-Round Proofs of Shuffle: Terelius-Wikstrom and Bayer-Groth .................................................. 6471
Thomas Haines, Australian National University; Rajeev Gore, Polish Academy of Science; Mukesh Tiwari, University of Cambridge

TAP: Transparent and Privacy-Preserving Data Services ................................................................. 6489
Daniel Reisbergen and Aung Maw, Singapore University of Technology and Design; Zheng Yang, Southwest University; Tien Tuan Anh Dinh and Jianying Zhou, Singapore University of Technology and Design

Vulnerabilities and Threat Detection

Trojan Source: Invisible Vulnerabilities .............................................. 6507
Nicholas Boucher, University of Cambridge; Ross Anderson, University of Cambridge and University of Edinburgh

Cheesecloth: Zero-Knowledge Proofs of Real World Vulnerabilities ............................................. 6525
Santiago Cuéllar, Bill Harris, James Parker, and Stuart Pernsteiner, Galois, Inc.; Eran Tromer, Columbia University

V1sCAn: Discovering 1-day Vulnerabilities in Reused C/C++ Open-source Software Components Using Code Classification Techniques ................................................. 6541
Seunghoon Woo, Eunjin Choi, Heejo Lee, and Hakjoo Oh, Korea University

VulChecker: Graph-based Vulnerability Localization in Source Code ................................................ 6557
Yisroel Mirsky, Ben-Gurion University of the Negev; George Macon, Georgia Tech Research Institute; Michael Brown, Georgia Institute of Technology; Carter Yagemann, Ohio State University; Matthew Pruett, Evan Downing, Sukarno Mertoguno, and Wenke Lee, Georgia Institute of Technology
**DISTDET: A Cost-Effective Distributed Cyber Threat Detection System.** .................................................. 6575
Feng Dong, School of Cyber Science and Engineering, Huazhong University of Science and Technology / Sangfor Technologies Inc.; Liu Wang and Xu Nie, Beijing University of Posts and Telecommunications; Fei Shao, Case Western Reserve University; Haoyu Wang, School of Cyber Science and Engineering, Huazhong University of Science and Technology; Ding Li, Key Laboratory of High-Confidence Software Technologies (MOE), School of Computer Science, Peking University; Xiapu Luo, The Hong Kong Polytechnic University; Xusheng Xiao, Arizona State University

**Automated Analysis of Deployed Systems**

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

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

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

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

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

**Manipulation, Influence, and Elections**

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

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

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

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

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

**Side Channel Attacks**

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

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

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

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

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

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

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

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

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

Language-Based Security

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

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

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

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

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

Browsers

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

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

RoB: Ransomware over Modern Web Browsers ..................................................................................................... 7073
Harun Oz, Ahmet Aris, and Abbas Acar, Cyber-Physical Systems Security Lab, Florida International University; Güliz Seray Tuncay, Google; Leonardo Babun and Selcuk Uluagac, Cyber-Physical Systems Security Lab, Florida International University
Pool-Party: Exploiting Browser Resource Pools for Web Tracking ............................................. 7091
Peter Snyder, Brave Software; Soroush Karami, University of Illinois at Chicago; Arthur Edelstein, Brave Software; Benjamin Livshits, Imperial College London; Hamed Haddadi, Brave Software and Imperial College of London

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

Speculation Doesn’t Pay
Ultimate SLH: Taking Speculative Load Hardening to the Next Level ........................................ 7125
Zhiyuan Zhang, The University of Adelaide; Gilles Barthe, MPI-SP and IMDEA Software Institute; Chitchanok Chuengsatiansup, The University of Melbourne; Peter Schwabe, MPI-SP and Radboud University; Yuval Yarom, The University of Adelaide

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Attacks on Deployed Cryptosystems

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

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

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

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

Attacking, Defending, and Analyzing

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

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

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

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