30th USENIX Security Symposium (USENIX Security'21)

Online
11-13 August 2021

Volume 1 of 6

ISBN: 978-1-7138-3440-3

Printed from e-media with permission by:

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

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

Copyright© (2021) by Usenix Association
All rights reserved.

Printed with permission by Curran Associates, Inc. (2022)

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

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

https://www.usenix.org/

Additional copies of this publication are available from:

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

30th USENIX Security Symposium
August 11–13, 2021

Wednesday, August 11

Usability: Authentication

Effect of Mood, Location, Trust, and Presence of Others on Video-Based Social Authentication 1
Cheng Guo and Brianne Campbell, *Clemson University;* Apu Kapadia, *Indiana University;* Michael K. Reiter, *Duke University;* Kelly Caine, *Clemson University*

'Passwords Keep Me Safe' – Understanding What Children Think about Passwords 19
Mary Theofanos and Yee-Yin Choong, *National Institute of Standards and Technology;* Olivia Murphy, *University of Maryland, College Park*

On the Usability of Authenticity Checks for Hardware Security Tokens 37
Katharina Pfeffer and Alexandra Mai, *SBA Research;* Adrian Dabrowski, *University of California, Irvine;* Matthias Gusenbauer, *Tokyo Institute of Technology & SBA Research;* Philipp Schindler, *SBA Research;* Edgar Weippl, *University of Vienna;* Michael Franz, *University of California, Irvine;* Katharina Krombholz, *CISPA Helmholtz Center for Information Security*

Inexpensive Brainwave Authentication: New Techniques and Insights on User Acceptance 55
Patricia Arias-Cabarcos, *KASTEL/KIT;* Thilo Habrich, Karen Becker, and Christian Becker, *University of Mannheim;* Thorsten Strufe, *KASTEL/KIT*

Why Older Adults (Don't) Use Password Managers 73
Hirak Ray, Flynn Wolf, and Ravi Kuber, *University of Maryland, Baltimore County;* Adam J. Aviv, *The George Washington University*

"*It's Stored, Hopefully, on an Encrypted Server*": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn 91
Leona Lassak, *Ruhr University Bochum;* Annika Hildebrandt, *University of Chicago;* Maximilian Golla, *Max Planck Institute for Security and Privacy;* Blase Ur, *University of Chicago*

Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns 109
Maximilian Golla, *Max Planck Institute for Security and Privacy;* Grant Ho, *University of California San Diego;* Marika Lohmus, *Cleo AI;* Monica Pulluri, *Facebook;* Elissa M. Redmiles, *Max Planck Institute for Software Systems*

Cryptography: Attacks

Hiding the Access Pattern is Not Enough: Exploiting Search Pattern Leakage in Searchable Encryption 127
Simon Oya and Florian Kerschbaum, *University of Waterloo*

A Highly Accurate Query-Recovery Attack against Searchable Encryption using Non-Indexed Documents 143
Marc Damie, *University of Technology of Compiègne, France;* Florian Hahn and Andreas Peter, *University of Twente, The Netherlands*

Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation 161
Mathy Vanhoef, *New York University Abu Dhabi*

Card Brand Mixup Attack: Bypassing the PIN in non-Visa Cards by Using Them for Visa Transactions 179
David Basin, Ralf Sasse, and Jorge Toro-Pozo, *Department of Computer Science, ETH Zurich*

Partitioning Oracle Attacks 195
Julia Len, Paul Grubbs, and Thomas Ristenpart, *Cornell Tech*

Raccoon Attack: Finding and Exploiting Most-Significant-Bit-Oracles in TLS-DH(E) 213
Robert Merget and Marcus Brinkmann, *Ruhr University Bochum;* Nimrod Aviram, *School of Computer Science, Tel Aviv University;* Juraj Somorovsky, *Paderborn University;* Johannes Mittmann, *Bundesamt für Sicherheit in der Informationstechnik* (*BSI*)*, Germany;* Jörg Schwenk, *Ruhr University Bochum*

A Side Journey To Titan 231
Thomas Roche and Victor Lomné, *NinjaLab, Montpellier, France;* Camille Mutschler, *NinjaLab, Montpellier, France and LIRMM, Univ. Montpellier, CNRS, Montpellier, France;* Laurent Imbert, *LIRMM, Univ. Montpellier, CNRS, Montpellier, France*

Embedded Security & SW Sec

PASan: Detecting Peripheral Access Concurrency Bugs within Bare-Metal Embedded Applications 249
Taegyu Kim, *Purdue University;* Vireshwar Kumar, *Indian Institute of Technology, Delhi;* Junghwan Rhee, *University of Central Oklahoma;* Jizhou Chen and Kyungtae Kim, *Purdue University;* Chung Hwan Kim, *University of Texas at Dallas;* Dongyan Xu and Dave (Jing) Tian, *Purdue University*

On the Design and Misuse of Microcoded (Embedded) Processors — A Cautionary Note 267
Nils Albartus and Clemens Nasenberg, *Ruhr University Bochum, Germany; Max Planck Institute for Security and Privacy, Germany;* Florian Stolz, *Ruhr University Bochum, Germany;* Marc Fyrbiak, *Max Planck Institute for Security and Privacy, Germany;* Christof Paar, *Ruhr University Bochum, Germany; Max Planck Institute for Security and Privacy, Germany;* Russell Tessier, *University of Massachusetts, Amherst, USA*

M2Mon: Building an MMIO-based Security Reference Monitor for Unmanned Vehicles 285
Arslan Khan and Hyungsub Kim, *Purdue University;* Byoungyoung Lee, *Seoul National University (SNU);* Dongyan Xu, Antonio Bianchi, and Dave (Jing) Tian, *Purdue University*

Sharing More and Checking Less: Leveraging Common Input Keywords to Detect Bugs in Embedded Systems . . 303
Libo Chen, *School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University;* Yanhao Wang, *QI-ANXIN Technology Research Institute;* Quanpu Cai and Yunfan Zhan, *School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University;* Hong Hu, *Pennsylvania State University;* Jiaqi Linghu, *QI-ANXIN Technology Research Institute;* Qinsheng Hou, *QI-ANXIN Technology Research Institute; Shandong University;* Chao Zhang and Haixin Duan, *BNRist & Institute for Network Science and Cyberspace, Tsinghua University; Tsinghua University-QI-ANXIN Group JCNS;* Zhi Xue, *School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University*

Jetset: Targeted Firmware Rehosting for Embedded Systems 321
Evan Johnson, *University of California, San Diego;* Maxwell Bland, YiFei Zhu, and Joshua Mason, *University of Illinois at Urbana–Champaign;* Stephen Checkoway, *Oberlin College;* Stefan Savage, *University of California, San Diego;* Kirill Levchenko, *University of Illinois at Urbana–Champaign*

LightBlue: Automatic Profile-Aware Debloating of Bluetooth Stacks 339
Jianliang Wu and Ruoyu Wu, *Purdue University;* Daniele Antonioli and Mathias Payer, *EPFL;* Nils Ole Tippenhauer, *CISPA Helmholtz Center for Information Security;* Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi, *Purdue University*

PACStack: an Authenticated Call Stack 357
Hans Liljestrand, *University of Waterloo;* Thomas Nyman and Lachlan J. Gunn, *Aalto University;* Jan-Erik Ekberg, *Huawei Technologies and Aalto University;* N. Asokan, *University of Waterloo and Aalto University*

Usable Security and Privacy: User Perspectives

"It's stressful having all these phones": Investigating Sex Workers' Safety Goals, Risks, and Practices Online 375
Allison McDonald, *University of Michigan;* Catherine Barwulor, *Clemson University;* Michelle L. Mazurek, *University of Maryland;* Florian Schaub, *University of Michigan;* Elissa M. Redmiles, *Max Planck Institute for Software Systems*

"Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them . . .393
Peter Mayer, *Karlsruhe Institute of Technology;* Yixin Zou and Florian Schaub, *University of Michigan;* Adam J. Aviv, *The George Washington University*

"It's the Company, the Government, You and I": User Perceptions of Responsibility for Smart Home Privacy and Security 411
Julie Haney, *National Institute of Standards and Technology;* Yasemin Acar, *National Institute of Standards and Technology and Leibniz University Hannover;* Susanne Furman, *National Institute of Standards and Technology*

The Role of Computer Security Customer Support in Helping Survivors of Intimate Partner Violence 429
Yixin Zou and Allison McDonald, *University of Michigan;* Julia Narakornpichit, Nicola Dell, and Thomas Ristenpart, *Cornell Tech;* Kevin Roundy, *Norton Research Group;* Florian Schaub, *University of Michigan;* Acar Tamersoy, *Norton Research Group*

Evaluating In-Workflow Messages for Improving Mental Models of End-to-End Encryption 447
Omer Akgul, Wei Bai, Shruti Das, and Michelle L. Mazurek, *University of Maryland*

PriSEC: A Privacy Settings Enforcement Controller 465
Rishabh Khandelwal and Thomas Linden, *University of Wisconsin–Madison;* Hamza Harkous, *Google Inc.;* Kassem Fawaz, *University of Wisconsin–Madison*

Are Privacy Dashboards Good for End Users? Evaluating User Perceptions and Reactions to Google's My Activity . . .483
Florian M. Farke, *Ruhr University Bochum;* David G. Balash, *The George Washington University;* Maximilian Golla, *Max Planck Institute for Security and Privacy;* Markus Dürmuth, *Ruhr University Bochum;* Adam J. Aviv, *The George Washington University*

Cryptographic Proof Systems, Analysis, and Applications

Mystique: Efficient Conversions for Zero-Knowledge Proofs with Applications to Machine Learning 501
Chenkai Weng, *Northwestern University;* Kang Yang, *State Key Laboratory of Cryptology;* Xiang Xie, *Shanghai Key Laboratory of Privacy-Preserving Computation and MatrixElements Technologies;* Jonathan Katz, *University of Maryland;* Xiao Wang, *Northwestern University*

Poseidon: A New Hash Function for Zero-Knowledge Proof Systems 519
Lorenzo Grassi, *Radboud University Nijmegen;* Dmitry Khovratovich, *Ethereum Foundation and Dusk Network;* Christian Rechberger, *IAIK, Graz University of Technology;* Arnab Roy, *University of Klagenfurt;* Markus Schofnegger, *IAIK, Graz University of Technology*

Dynamic proofs of retrievability with low server storage 537
Gaspard Anthoine, Jean-Guillaume Dumas, Mélanie de Jonghe, Aude Maignan, and Clément Pernet, *Université Grenoble Alpes;* Michael Hanling and Daniel S. Roche, *United States Naval Academy*

Where's Crypto?: Automated Identification and Classification of Proprietary Cryptographic Primitives in Binary Code 555
Carlo Meijer, *Radboud University;* Veelasha Moonsamy, *Ruhr University Bochum;* Jos Wetzels, *Midnight Blue Labs*

Towards Formal Verification of State Continuity for Enclave Programs 573
Mohit Kumar Jangid, *The Ohio State University;* Guoxing Chen, *Shanghai Jiao Tong University;* Yinqian Zhang, *Southern University of Science and Technology;* Zhiqiang Lin, *The Ohio State University*

Protecting Cryptography Against Compelled Self-Incrimination 591
Sarah Scheffler and Mayank Varia, *Boston University*

CSProp: Ciphertext and Signature Propagation Low-Overhead Public-Key Cryptosystem for IoT Environments . . . 609
Fatemah Alharbi, *Taibah University, Yanbu;* Arwa Alrawais, *Prince Sattam Bin Abdulaziz University;* Abdulrahman Bin Rabiah, *University of California, Riverside, and King Saud University;* Silas Richelson and Nael Abu-Ghazaleh, *University of California, Riverside*

Hardware Side Channel Attacks

Automatic Extraction of Secrets from the Transistor Jungle using Laser-Assisted Side-Channel Attacks 627
Thilo Krachenfels and Tuba Kiyan, *Technische Universität Berlin;* Shahin Tajik, *Worcester Polytechnic Institute;* Jean-Pierre Seifert, *Technische Universität Berlin; Fraunhofer SIT*

Lord of the Ring(s): Side Channel Attacks on the CPU On-Chip Ring Interconnect Are Practical 645
Riccardo Paccagnella, Licheng Luo, and Christopher W. Fletcher, *University of Illinois at Urbana-Champaign*

Frontal Attack: Leaking Control-Flow in SGX via the CPU Frontend 663
Ivan Puddu, Moritz Schneider, Miro Haller, and Srdjan Čapkun, *ETH Zurich*

Charger-Surfing: Exploiting a Power Line Side-Channel for Smartphone Information Leakage 681
Patrick Cronin, Xing Gao, and Chengmo Yang, *University of Delaware;* Haining Wang, *Virginia Tech*

VoltPillager: Hardware-based fault injection attacks against Intel SGX Enclaves using the SVID voltage scaling interface 699
Zitai Chen, Georgios Vasilakis, Kit Murdock, Edward Dean, David Oswald, and Flavio D. Garcia, *School of Computer Science, University of Birmingham, UK*

CipherLeaks: Breaking Constant-time Cryptography on AMD SEV via the Ciphertext Side Channel 717
Mengyuan Li, *The Ohio State University;* Yinqian Zhang, *Southern University of Science and Technology;* Huibo Wang and Kang Li, *Baidu Security;* Yueqiang Cheng, *NIO Security Research*

Cross-VM and Cross-Processor Covert Channels Exploiting Processor Idle Power Management 733
Paizhuo Chen, Lei Li, and Zhice Yang, *ShanghaiTech University*

Permissions and Passwords

Can Systems Explain Permissions Better? Understanding Users' Misperceptions under Smartphone Runtime Permission Model 751
Bingyu Shen, *University of California, San Diego;* Lili Wei, *The Hong Kong University of Science and Technology;* Chengcheng Xiang, Yudong Wu, Mingyao Shen, and Yuanyuan Zhou, *University of California, San Diego;* Xinxin Jin, *Whova, Inc.*

"Shhh. be quiet!" Reducing the Unwanted Interruptions of Notification Permission Prompts on Chrome 769
Igor Bilogrevic, Balazs Engedy, Judson L. Porter III, Nina Taft, Kamila Hasanbega, Andrew Paseltiner, Hwi Kyoung Lee, Edward Jung, Meggyn Watkins, PJ McLachlan, and Jason James, *Google*

Explanation Beats Context: The Effect of Timing & Rationales on Users' Runtime Permission Decisions 785
Yusra Elbitar, *CISPA Helmholtz Center for Information Security, Saarland University;* Michael Schilling, *CISPA Helmholtz Center for Information Security;* Trung Tin Nguyen, *CISPA Helmholtz Center for Information Security, Saarland University;* Michael Backes and Sven Bugiel, *CISPA Helmholtz Center for Information Security*

A Large Scale Study of User Behavior, Expectations and Engagement with Android Permissions 803
Weicheng Cao and Chunqiu Xia, *University of Toronto;* Sai Teja Peddinti, *Google;* David Lie, *University of Toronto;* Nina Taft, *Google;* Lisa M. Austin, *University of Toronto*

Reducing Bias in Modeling Real-world Password Strength via Deep Learning and Dynamic Dictionaries 821
Dario Pasquini, *Sapienza University of Rome, Institute of Applied Computing CNR;* Marco Cianfriglia, *Institute of Applied Computing CNR;* Giuseppe Ateniese, *Stevens Institute of Technology;* Massimo Bernaschi, *Institute of Applied Computing CNR*

Using Amnesia to Detect Credential Database Breaches 839
Ke Coby Wang, *University of North Carolina at Chapel Hill;* Michael K. Reiter, *Duke University*

Incrementally Updateable Honey Password Vaults 857
Haibo Cheng, Wenting Li, and Ping Wang, *Peking University;* Chao-Hsien Chu, *Pennsylvania State University;* Kaitai Liang, *Delft University of Technology*

Private Computation and Differential Privacy

Private Blocklist Lookups with Checklist 875
Dmitry Kogan, *Stanford University;* Henry Corrigan-Gibbs, *MIT CSAIL*

Identifying Harmful Media in End-to-End Encrypted Communication: Efficient Private Membership Computation 893
Anunay Kulshrestha and Jonathan Mayer, *Princeton University*

Fuzzy Labeled Private Set Intersection with Applications to Private Real-Time Biometric Search 911
Erkam Uzun, Simon P. Chung, Vladimir Kolesnikov, Alexandra Boldyreva, and Wenke Lee, *Georgia Institute of Technology*

PrivSyn: Differentially Private Data Synthesis 929
Zhikun Zhang, *Zhejiang University and CISPA Helmholtz Center for Information Security;* Tianhao Wang, Ninghui Li, and Jean Honorio, *Purdue University;* Michael Backes, *CISPA Helmholtz Center for Information Security;* Shibo He and Jiming Chen, *Zhejiang University and Alibaba-Zhejiang University Joint Research Institute of Frontier Technologies;* Yang Zhang, *CISPA Helmholtz Center for Information Security*

Data Poisoning Attacks to Local Differential Privacy Protocols 947
Xiaoyu Cao, Jinyuan Jia, and Neil Zhenqiang Gong, *Duke University*

How to Make Private Distributed Cardinality Estimation Practical, and Get Differential Privacy for Free 965
Changhui Hu, *Newcastle University;* Jin Li, *Guangzhou University;* Zheli Liu, Xiaojie Guo, Yu Wei, and Xuan Guang, *Nankai University;* Grigorios Loukides, *King's College London;* Changyu Dong, *Newcastle University*

Locally Differentially Private Analysis of Graph Statistics 983
Jacob Imola, *UC San Diego;* Takao Murakami, *AIST;* Kamalika Chaudhuri, *UC San Diego*

Hardware Security

SMASH: Synchronized Many-sided Rowhammer Attacks from JavaScript 1001
Finn de Ridder, *ETH Zurich and VU Amsterdam;* Pietro Frigo, Emanuele Vannacci, Herbert Bos, and Cristiano Giuffrida, *VU Amsterdam;* Kaveh Razavi, *ETH Zurich*

Database Reconstruction from Noisy Volumes: A Cache Side-Channel Attack on SQLite 1019
Aria Shahverdi, *University of Maryland;* Mahammad Shirinov, *Bilkent University;* Dana Dachman-Soled, *University of Maryland*

PTAuth: Temporal Memory Safety via Robust Points-to Authentication. 1037
Reza Mirzazade Farkhani, Mansour Ahmadi, and Long Lu, *Northeastern University*

Does logic locking work with EDA tools? 1055
Zhaokun Han, Muhammad Yasin, and Jeyavijayan (JV) Rajendran, *Texas A&M University*

CURE: A Security Architecture with CUstomizable and Resilient Enclaves 1073
Raad Bahmani, Ferdinand Brasser, Ghada Dessouky, Patrick Jauernig, Matthias Klimmek, Ahmad-Reza Sadeghi, and Emmanuel Stapf, *Technische Universität Darmstadt*

DICE*: A Formally Verified Implementation of DICE Measured Boot 1091
Zhe Tao, *University of California, Davis;* Aseem Rastogi, Naman Gupta, and Kapil Vaswani, *Microsoft Research;* Aditya V. Thakur, *University of California, Davis*

PEARL: Plausibly Deniable Flash Translation Layer using WOM coding 1109
Chen Chen, Anrin Chakraborti, and Radu Sion, *Stony Brook University*

Usable Security and Privacy: Institutional Perspectives

Examining the Efficacy of Decoy-based and Psychological Cyber Deception 1127
Kimberly J. Ferguson-Walter, *Laboratory for Advanced Cybersecurity Research;* Maxine M. Major, *Naval Information Warfare Center, Pacific;* Chelsea K. Johnson, *Arizona State University;* Daniel H. Muhleman, *Naval Information Warfare Center, Pacific*

Helping Users Automatically Find and Manage Sensitive, Expendable Files in Cloud Storage. 1145
Mohammad Taha Khan, *University of Illinois at Chicago / Washington & Lee University;* Christopher Tran and Shubham Singh, *University of Illinois at Chicago;* Dimitri Vasilkov, *University of Chicago;* Chris Kanich, *University of Illinois at Chicago;* Blase Ur, *University of Chicago;* Elena Zheleva, *University of Illinois at Chicago*

Adapting Security Warnings to Counter Online Disinformation 1163
Ben Kaiser, Jerry Wei, Elena Lucherini, and Kevin Lee, *Princeton University;* J. Nathan Matias, *Cornell University;* Jonathan Mayer, *Princeton University*

"Why wouldn't someone think of democracy as a target?": Security practices & challenges of people involved with U.S. political campaigns 1181
Sunny Consolvo, Patrick Gage Kelley, Tara Matthews, Kurt Thomas, Lee Dunn, and Elie Bursztein, *Google*

Security Obstacles and Motivations for Small Businesses from a CISO's Perspective 1199
Flynn Wolf, *University of Maryland, Baltimore County;* Adam J. Aviv, *The George Washington University;* Ravi Kuber, *University of Maryland, Baltimore County*

Strategies and Perceived Risks of Sending Sensitive Documents. 1217
Noel Warford, *University of Maryland;* Collins W. Munyendo, *The George Washington University;* Ashna Mediratta, *University of Maryland;* Adam J. Aviv, *The George Washington University;* Michelle L. Mazurek, *University of Maryland*

A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises. 1235
Nicolas Huaman, *Leibniz University Hannover; CISPA Helmholtz Center for Information Security;* Bennet von Skarczinski, *PwC Germany;* Christian Stransky and Dominik Wermke, *Leibniz University Hannover;* Yasemin Acar, *Leibniz University Hannover; Max Planck Institute for Security and Privacy;* Arne Dreißigacker, *Criminological Research Institute of Lower Saxony;* Sascha Fahl, *Leibniz University Hannover; CISPA Helmholtz Center for Information Security*

Cryptocurrencies and Smart Contracts

On the Routing-Aware Peering against Network-Eclipse Attacks in Bitcoin 1253
Muoi Tran and Akshaye Shenoi, *National University of Singapore;* Min Suk Kang, *KAIST*

EOSafe: Security Analysis of EOSIO Smart Contracts 1271
Ningyu He, *Key Lab on HCST* (*MOE*)*, Peking University;* Ruiyi Zhang, *PeckShield, Inc.;* Haoyu Wang, *Beijing University of Posts and Telecommunications;* Lei Wu, *Zhejiang University;* Xiapu Luo, *The Hong Kong Polytechnic University;* Yao Guo, *Key Lab on HCST* (*MOE*)*, Peking University;* Ting Yu, *Qatar Computing Research Institute;* Xuxian Jiang, *PeckShield, Inc.*

EVMPatch: Timely and Automated Patching of Ethereum Smart Contracts 1289
Michael Rodler, *University of Duisburg-Essen;* Wenting Li and Ghassan O. Karame, *NEC Laboratories Europe;* Lucas Davi, *University of Duisburg-Essen*

Evil Under the Sun: Understanding and Discovering Attacks on Ethereum Decentralized Applications 1307
Liya Su, *Indiana University Bloomington; Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences;* Xinyue Shen, *Indiana University Bloomington and Alibaba Group;* Xiangyu Du, *Indiana University Bloomington; Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences;* Xiaojing Liao, XiaoFeng Wang, and Luyi Xing, *Indiana University Bloomington;* Baoxu Liu, *Institute of Information Engineering, Chinese Academy of Sciences; University of Chinese Academy of Sciences*

Smart Contract Vulnerabilities: Vulnerable Does Not Imply Exploited 1325
Daniel Perez and Benjamin Livshits, *Imperial College London*

Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain 1343
Christof Ferreira Torres, *SnT, University of Luxembourg;* Ramiro Camino, *Luxembourg Institute of Science and Technology;* Radu State, *SnT, University of Luxembourg*

SmarTest: Effectively Hunting Vulnerable Transaction Sequences in Smart Contracts through Language Model-Guided Symbolic Execution 1361
Sunbeom So, Seongjoon Hong, and Hakjoo Oh, *Korea University*

Hardware Side Channel Defenses

MIRAGE: Mitigating Conflict-Based Cache Attacks with a Practical Fully-Associative Design 1379
Gururaj Saileshwar and Moinuddin Qureshi, *Georgia Institute of Technology*

Dolma: Securing Speculation with the Principle of Transient Non-Observability 1397
Kevin Loughlin, Ian Neal, Jiacheng Ma, Elisa Tsai, Ofir Weisse, Satish Narayanasamy, and Baris Kasikci, *University of Michigan*

Osiris: Automated Discovery of Microarchitectural Side Channels 1415
Daniel Weber, Ahmad Ibrahim, Hamed Nemati, Michael Schwarz, and Christian Rossow, *CISPA Helmholtz Center for Information Security*

Swivel: Hardening WebAssembly against Spectre 1433
Shravan Narayan and Craig Disselkoen, *UC San Diego;* Daniel Moghimi, *Worcester Polytechnic Institute and UC San Diego;* Sunjay Cauligi, Evan Johnson, and Zhao Gang, *UC San Diego;* Anjo Vahldiek-Oberwagner, *Intel Labs;* Ravi Sahita, *Intel;* Hovav Shacham, *UT Austin;* Dean Tullsen and Deian Stefan, *UC San Diego*

Rage Against the Machine Clear: A Systematic Analysis of Machine Clears and Their Implications for Transient Execution Attacks 1451
Hany Ragab, Enrico Barberis, Herbert Bos, and Cristiano Giuffrida, *Vrije Universiteit Amsterdam*

Coco: Co-Design and Co-Verification of Masked Software Implementations on CPUs 1469
Barbara Gigerl, Vedad Hadzic, and Robert Primas, *Graz University of Technology;* Stefan Mangard, *Graz University of Technology, Lamarr Security Research;* Roderick Bloem, *Graz University of Technology*

Thursday, August 12

Machine Learning: Backdoor and Poisoning

Explanation-Guided Backdoor Poisoning Attacks Against Malware Classifiers 1487
Giorgio Severi, *Northeastern University;* Jim Meyer, *Xailient Inc.;* Scott Coull, *FireEye Inc.;* Alina Oprea, *Northeastern University*

Blind Backdoors in Deep Learning Models 1505
Eugene Bagdasaryan and Vitaly Shmatikov, *Cornell Tech*

Graph Backdoor 1523
Zhaohan Xi and Ren Pang, *Pennsylvania State University;* Shouling Ji, *Zhejiang University;* Ting Wang, *Pennsylvania State University*

Demon in the Variant: Statistical Analysis of DNNs for Robust Backdoor Contamination Detection 1541
Di Tang, *Chinese University of Hong Kong;* XiaoFeng Wang and Haixu Tang, *Indiana University;* Kehuan Zhang, *Chinese University of Hong Kong*

You Autocomplete Me: Poisoning Vulnerabilities in Neural Code Completion 1559
Roei Schuster, *Tel-Aviv University, Cornell Tech;* Congzheng Song, *Cornell University;* Eran Tromer, *Tel Aviv University;* Vitaly Shmatikov, *Cornell Tech*

Poisoning the Unlabeled Dataset of Semi-Supervised Learning 1577
Nicholas Carlini, *Google*

Double-Cross Attacks: Subverting Active Learning Systems 1593
Jose Rodrigo Sanchez Vicarte, Gang Wang, and Christopher W. Fletcher, *University of Illinois at Urbana-Champaign*

Program Analysis

Fine Grained Dataflow Tracking with Proximal Gradients 1611
Gabriel Ryan, Abhishek Shah, and Dongdong She, *Columbia University;* Koustubha Bhat, *Vrije Universiteit Amsterdam;* Suman Jana, *Columbia University*

Static Detection of Unsafe DMA Accesses in Device Drivers 1629
Jia-Ju Bai and Tuo Li, *Tsinghua University;* Kangjie Lu, *University of Minnesota;* Shi-Min Hu, *Tsinghua University*

MAZE: Towards Automated Heap Feng Shui 1647
Yan Wang, *{CAS-KLONAT, BKLONSPT}, Institute of Information Engineering, Chinese Academy of Sciences; WeiRan Lab, Huawei Technologies;* Chao Zhang, *BNRist & Institute for Network Science and Cyberspace, Tsinghua University; Tsinghua University-QI-ANXIN Group JCNS;* Zixuan Zhao, Bolun Zhang, Xiaorui Gong, and Wei Zou, *{CAS-KLONAT, BKLONSPT,} Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences*

SELECTIVETAINT: Efficient Data Flow Tracking With Static Binary Rewriting 1665
Sanchuan Chen, Zhiqiang Lin, and Yinqian Zhang, *The Ohio State University*

Breaking Through Binaries: Compiler-quality Instrumentation for Better Binary-only Fuzzing 1683
Stefan Nagy, *Virginia Tech;* Anh Nguyen-Tuong, Jason D. Hiser, and Jack W. Davidson, *University of Virginia;* Matthew Hicks, *Virginia Tech*

MBA-Blast: Unveiling and Simplifying Mixed Boolean-Arithmetic Obfuscation 1701
Binbin Liu, *University of Science and Technology of China & University of New Hampshire;* Junfu Shen, *University of New Hampshire;* Jiang Ming, *University of Texas at Arlington;* Qilong Zheng and Jing Li, *University of Science and Technology of China;* Dongpeng Xu, *University of New Hampshire*

VScape: Assessing and Escaping Virtual Call Protections 1719
Kaixiang Chen, *Institute for Network Science and Cyberspace, Tsinghua University;* Chao Zhang, *Institute for Network Science and Cyberspace, Tsinghua University/Beijing National Research Center for Information Science and Technology/ Tsinghua University-QI-ANXIN Group JCNS;* Tingting Yin and Xingman Chen, *Institute for Network Science and Cyberspace, Tsinghua University;* Lei Zhao, *School of Cyber Science and Engineering, Wuhan University*

Privacy Enhancing Technologies

Pretty Good Phone Privacy 1737
Paul Schmitt, *Princeton University;* Barath Raghavan, *University of Southern California*

KeyForge: Non-Attributable Email from Forward-Forgeable Signatures 1755
Michael A. Specter, *MIT;* Sunoo Park, *MIT & Harvard;* Matthew Green, *Johns Hopkins University*

Express: Lowering the Cost of Metadata-hiding Communication with Cryptographic Privacy 1775
Saba Eskandarian, *Stanford University;* Henry Corrigan-Gibbs, *MIT CSAIL;* Matei Zaharia and Dan Boneh, *Stanford University*

Kalɛido: Real-Time Privacy Control for Eye-Tracking Systems 1793
Jingjie Li, Amrita Roy Chowdhury, Kassem Fawaz, and Younghyun Kim, *University of Wisconsin–Madison*

Communication–Computation Trade-offs in PIR. 1811
Asra Ali, *Google;* Tancrède Lepoint*;* Sarvar Patel, Mariana Raykova, Phillipp Schoppmann, Karn Seth, and Kevin Yeo, *Google*

I Always Feel Like Somebody's Sensing Me! A Framework to Detect, Identify, and Localize Clandestine Wireless Sensors 1829
Akash Deep Singh, *University of California, Los Angeles;* Luis Garcia, *University of California, Los Angeles, and USC ISI;* Joseph Noor and Mani Srivastava, *University of California, Los Angeles*

The Complexities of Healing in Secure Group Messaging: Why Cross-Group Effects Matter 1847
Cas Cremers, *CISPA Helmholtz Center for Information Security;* Britta Hale, *Naval Postgraduate School* (*NPS*)*;* Konrad Kohbrok, *Aalto University*

Machine Learning: Adversarial Examples and Model Extraction

SLAP: Improving Physical Adversarial Examples with Short-Lived Adversarial Perturbations 1865
Giulio Lovisotto, Henry Turner, and Ivo Sluganovic, *University of Oxford;* Martin Strohmeier, *armasuisse;* Ivan Martinovic, *University of Oxford*

Adversarial Policy Training against Deep Reinforcement Learning 1883
Xian Wu, Wenbo Guo, Hua Wei, and Xinyu Xing, *The Pennsylvania State University*

DRMI: A Dataset Reduction Technology based on Mutual Information for Black-box Attacks 1901
Yingzhe He, Guozhu Meng, Kai Chen, Xingbo Hu, and Jinwen He, *SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences/School of Cyber Security, University of Chinese Academy of Sciences*

Deep-Dup: An Adversarial Weight Duplication Attack Framework to Crush Deep Neural Network in Multi-Tenant FPGA 1919
Adnan Siraj Rakin, *Arizona State University;* Yukui Luo and Xiaolin Xu, *Northeastern University;* Deliang Fan, *Arizona State University*

Entangled Watermarks as a Defense against Model Extraction 1937
Hengrui Jia and Christopher A. Choquette-Choo, *University of Toronto and Vector Institute;* Varun Chandrasekaran, *University of Wisconsin-Madison;* Nicolas Papernot, *University of Toronto and Vector Institute*

Mind Your Weight(s): A Large-scale Study on Insufficient Machine Learning Model Protection in Mobile Apps. . . 1955
Zhichuang Sun, Ruimin Sun, Long Lu, and Alan Mislove, *Northeastern University*

Hermes Attack: Steal DNN Models with Lossless Inference Accuracy. 1973
Yuankun Zhu, *The University of Texas at Dallas;* Yueqiang Cheng, *Baidu Security;* Husheng Zhou, *VMware;* Yantao Lu, *Syracuse University*

Automated Security Analysis of Source Code and Binaries

ARCUS: Symbolic Root Cause Analysis of Exploits in Production Systems 1989
Carter Yagemann, *Georgia Institute of Technology;* Matthew Pruett, *Georgia Tech Research Institute;* Simon P. Chung, *Georgia Institute of Technology;* Kennon Bittick, *Georgia Tech Research Institute;* Brendan Saltaformaggio and Wenke Lee, *Georgia Institute of Technology*

Automatic Firmware Emulation through Invalidity-guided Knowledge Inference **2007**
Wei Zhou, *National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences;* Le Guan, *Department of Computer Science, University of Georgia;* Peng Liu, *College of Information Sciences and Technology, The Pennsylvania State University;* Yuqing Zhang, *National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences; School of Cyber Engineering, Xidian University; School of Computer Science and Cyberspace Security, Hainan University*

Finding Bugs Using Your Own Code: Detecting Functionally-similar yet Inconsistent Code **2025**
Mansour Ahmadi, Reza Mirzazade Farkhani, Ryan Williams, and Long Lu, *Northeastern University*

Understanding and Detecting Disordered Error Handling with Precise Function Pairing **2041**
Qiushi Wu, Aditya Pakki, Navid Emamdoost, Stephen McCamant, and Kangjie Lu, *University of Minnesota*

Precise and Scalable Detection of Use-after-Compacting-Garbage-Collection Bugs **2059**
HyungSeok Han, Andrew Wesie, and Brian Pak, *Theori Inc.*

Reducing Test Cases with Attention Mechanism of Neural Networks **2075**
Xing Zhang, Jiongyi Chen, Chao Feng, Ruilin Li, Yunfei Su, Bin Zhang, Jing Lei, and Chaojing Tang, *National University of Defense Technology*

FlowDist: Multi-Staged Refinement-Based Dynamic Information Flow Analysis for Distributed Software Systems **2093**
Xiaoqin Fu and Haipeng Cai, *Washington State University, Pullman, WA*

Secure Multiparty Computation

Privacy and Integrity Preserving Computations with CRISP **2111**
Sylvain Chatel, Apostolos Pyrgelis, Juan Ramón Troncoso-Pastoriza, and Jean-Pierre Hubaux, *EPFL*

Senate: A Maliciously-Secure MPC Platform for Collaborative Analytics **2129**
Rishabh Poddar and Sukrit Kalra, *UC Berkeley;* Avishay Yanai, *VMware Research;* Ryan Deng, Raluca Ada Popa, and Joseph M. Hellerstein, *UC Berkeley*

GForce: GPU-Friendly Oblivious and Rapid Neural Network Inference **2147**
Lucien K. L. Ng and Sherman S. M. Chow, *The Chinese University of Hong Kong, Hong Kong*

ABY2.0: Improved Mixed-Protocol Secure Two-Party Computation **2165**
Arpita Patra, *Indian Institute of Science;* Thomas Schneider, *TU Darmstadt;* Ajith Suresh, *Indian Institute of Science;* Hossein Yalame, *TU Darmstadt*

Fantastic Four: Honest-Majority Four-Party Secure Computation With Malicious Security **2183**
Anders Dalskov, *Aarhus University & Partisia;* Daniel Escudero, *Aarhus University;* Marcel Keller, *CSIRO's Data61*

Muse: Secure Inference Resilient to Malicious Clients **2201**
Ryan Lehmkuhl and Pratyush Mishra, *UC Berkeley;* Akshayaram Srinivasan, *Tata Institute of Fundamental Research;* Raluca Ada Popa, *UC Berkeley*

ObliCheck: Efficient Verification of Oblivious Algorithms with Unobservable State **2219**
Jeongseok Son, Griffin Prechter, Rishabh Poddar, Raluca Ada Popa, and Koushik Sen, *University of California, Berkeley*

Adversarial Machine Learning: Defenses

PatchGuard: A Provably Robust Defense against Adversarial Patches via Small Receptive Fields and Masking . **2237**
Chong Xiang, *Princeton University;* Arjun Nitin Bhagoji, *University of Chicago;* Vikash Sehwag and Prateek Mittal, *Princeton University*

T-Miner: A Generative Approach to Defend Against Trojan Attacks on DNN-based Text Classification **2255**
Ahmadreza Azizi and Ibrahim Asadullah Tahmid, *Virginia Tech;* Asim Waheed, *LUMS Pakistan;* Neal Mangaokar, *University of Michigan;* Jiameng Pu, *Virginia Tech;* Mobin Javed, *LUMS Pakistan;* Chandan K. Reddy and Bimal Viswanath, *Virginia Tech*

WaveGuard: Understanding and Mitigating Audio Adversarial Examples **2273**
Shehzeen Hussain, Paarth Neekhara, Shlomo Dubnov, Julian McAuley, and Farinaz Koushanfar, *University of California, San Diego*

Cost-Aware Robust Tree Ensembles for Security Applications **2291**
Yizheng Chen, Shiqi Wang, Weifan Jiang, Asaf Cidon, and Suman Jana, *Columbia University*

DOMPTEUR: Taming Audio Adversarial Examples **2309**
Thorsten Eisenhofer, Lea Schönherr, and Joel Frank, *Ruhr University Bochum;* Lars Speckemeier, *University College London;* Dorothea Kolossa and Thorsten Holz, *Ruhr University Bochum*

CADE: Detecting and Explaining Concept Drift Samples for Security Applications **2327**
Limin Yang, *University of Illinois at Urbana-Champaign;* Wenbo Guo, *The Pennsylvania State University;* Qingying Hao, *University of Illinois at Urbana-Champaign;* Arridhana Ciptadi and Ali Ahmadzadeh, *Blue Hexagon;* Xinyu Xing, *The Pennsylvania State University;* Gang Wang, *University of Illinois at Urbana-Champaign*

SIGL: Securing Software Installations Through Deep Graph Learning **2345**
Xueyuan Han, *Harvard University;* Xiao Yu, *NEC Laboratories America;* Thomas Pasquier, *University of Bristol;* Ding Li, *Peking University;* Junghwan Rhee, *NEC Laboratories America;* James Mickens, *Harvard University;* Margo Seltzer, *University of British Columbia;* Haifeng Chen, *NEC Laboratories America*

Operating Systems Security

EXPRACE: Exploiting Kernel Races through Raising Interrupts **2363**
Yoochan Lee, *Seoul National University;* Changwoo Min, *Virginia Tech;* Byoungyoung Lee, *Seoul National University*

Undo Workarounds for Kernel Bugs **2381**
Seyed Mohammadjavad Seyed Talebi, Zhihao Yao, and Ardalan Amiri Sani, *UC Irvine;* Zhiyun Qian, *UC Riverside;* Daniel Austin, *Atlassian*

An Analysis of Speculative Type Confusion Vulnerabilities in the Wild **2399**
Ofek Kirzner and Adam Morrison, *Tel Aviv University*

Blinder: Partition-Oblivious Hierarchical Scheduling **2417**
Man-Ki Yoon, Mengqi Liu, Hao Chen, Jung-Eun Kim, and Zhong Shao, *Yale University*

SHARD: Fine-Grained Kernel Specialization with Context-Aware Hardening **2435**
Muhammad Abubakar, Adil Ahmad, Pedro Fonseca, and Dongyan Xu, *Purdue University*

Preventing Use-After-Free Attacks with Fast Forward Allocation **2453**
Brian Wickman, *GTRI;* Hong Hu, *PennState;* Insu Yun, Daehee Jang, and JungWon Lim, *GeorgiaTech;* Sanidhya Kashyap, *EPFL;* Taesoo Kim, *GeorgiaTech*

Detecting Kernel Refcount Bugs with Two-Dimensional Consistency Checking **2471**
Xin Tan, Yuan Zhang, and Xiyu Yang, *Fudan University;* Kangjie Lu, *University of Minnesota;* Min Yang, *Fudan University*

Web Security 1; Software Security

Effective Notification Campaigns on the Web: A Matter of Trust, Framing, and Support **2489**
Max Maass and Alina Stöver, *TU Darmstadt;* Henning Pridöhl, *Universität Bamberg;* Sebastian Bretthauer, *Goethe-Universität Frankfurt;* Dominik Herrmann, *Universität Bamberg;* Matthias Hollick, *TU Darmstadt;* Indra Spiecker, *Goethe-Universität Frankfurt*

Fingerprinting in Style: Detecting Browser Extensions via Injected Style Sheets **2507**
Pierre Laperdrix, *Univ. Lille, CNRS, Inria;* Oleksii Starov, *Palo Alto Networks;* Quan Chen and Alexandros Kapravelos, *North Carolina State University;* Nick Nikiforakis, *Stony Brook University*

JAW: Studying Client-side CSRF with Hybrid Property Graphs and Declarative Traversals **2525**
Soheil Khodayari and Giancarlo Pellegrino, *CISPA Helmholtz Center for Information Security*

AdCube: WebVR Ad Fraud and Practical Confinement of Third-Party Ads **2543**
Hyunjoo Lee, Jiyeon Lee, and Daejun Kim, *Korea Advanced Institute of Science and Technology;* Suman Jana, *Columbia University;* Insik Shin and Sooel Son, *Korea Advanced Institute of Science and Technology*

CACTI: Captcha Avoidance via Client-side TEE Integration **2561**
Yoshimichi Nakatsuka and Ercan Ozturk, *University of California, Irvine;* Andrew Paverd, *Microsoft Research;* Gene Tsudik, *University of California, Irvine*

PolyScope: Multi-Policy Access Control Analysis to Compute Authorized Attack Operations in Android Systems . . . 2579
Yu-Tsung Lee, *Penn State University;* William Enck, *North Carolina State University;* Haining Chen, *Google;* Hayawardh Vijayakumar, *Samsung Research;* Ninghui Li, *Purdue University;* Zhiyun Qian and Daimeng Wang, *UC Riverside;* Giuseppe Petracca, *Lyft;* Trent Jaeger, *Penn State University*

NYX: Greybox Hypervisor Fuzzing using Fast Snapshots and Affine Types 2597
Sergej Schumilo, Cornelius Aschermann, Ali Abbasi, Simon Wörner, and Thorsten Holz, *Ruhr-Universität Bochum*

Machine Learning: Privacy Issues

Systematic Evaluation of Privacy Risks of Machine Learning Models 2615
Liwei Song and Prateek Mittal, *Princeton University*

Extracting Training Data from Large Language Models 2633
Nicholas Carlini, *Google;* Florian Tramèr, *Stanford University;* Eric Wallace, *UC Berkeley;* Matthew Jagielski, *Northeastern University;* Ariel Herbert-Voss, *OpenAI and Harvard University;* Katherine Lee and Adam Roberts, *Google;* Tom Brown, *OpenAI;* Dawn Song, *UC Berkeley;* Úlfar Erlingsson, *Apple;* Alina Oprea, *Northeastern University;* Colin Raffel, *Google*

SWIFT: Super-fast and Robust Privacy-Preserving Machine Learning 2651
Nishat Koti, Mahak Pancholi, Arpita Patra, and Ajith Suresh, *Indian Institute of Science, Bangalore*

Stealing Links from Graph Neural Networks 2669
Xinlei He, *CISPA Helmholtz Center for Information Security;* Jinyuan Jia, *Duke University;* Michael Backes, *CISPA Helmholtz Center for Information Security;* Neil Zhenqiang Gong, *Duke University;* Yang Zhang, *CISPA Helmholtz Center for Information Security*

Leakage of Dataset Properties in Multi-Party Machine Learning 2687
Wanrong Zhang, *Georgia Institute of Technology;* Shruti Tople, *Microsoft Research;* Olga Ohrimenko, *The University of Melbourne*

Defeating DNN-Based Traffic Analysis Systems in Real-Time With Blind Adversarial Perturbations 2705
Milad Nasr, Alireza Bahramali, and Amir Houmansadr, *University of Massachusetts Amherst*

Cerebro: A Platform for Multi-Party Cryptographic Collaborative Learning 2723
Wenting Zheng, *UC Berkeley/CMU;* Ryan Deng, Weikeng Chen, and Raluca Ada Popa, *UC Berkeley;* Aurojit Panda, *New York University;* Ion Stoica, *UC Berkeley*

Fuzzing

SYZVEGAS: Beating Kernel Fuzzing Odds with Reinforcement Learning 2741
Daimeng Wang, Zheng Zhang, Hang Zhang, Zhiyun Qian, Srikanth V. Krishnamurthy, and Nael Abu-Ghazaleh, *University of California, Riverside*

Android SmartTVs Vulnerability Discovery via Log-Guided Fuzzing 2759
Yousra Aafer, *University of Waterloo;* Wei You, *Renmin University of China;* Yi Sun, Yu Shi, and Xiangyu Zhang, *Purdue University;* Heng Yin, *UC Riverside*

UNIFUZZ: A Holistic and Pragmatic Metrics-Driven Platform for Evaluating Fuzzers 2777
Yuwei Li, *Zhejiang University;* Shouling Ji, *Zhejiang University/Zhejiang University NGICS Platform;* Yuan Chen, *Zhejiang University;* Sizhuang Liang, *Georgia Institute of Technology;* Wei-Han Lee, *IBM Research;* Yueyao Chen and Chenyang Lyu, *Zhejiang University;* Chunming Wu, *Zhejiang University/Zhejiang Lab, Hangzhou, China;* Raheem Beyah, *Georgia Institute of Technology;* Peng Cheng, *Zhejiang University NGICS Platform/Zhejiang University;* Kangjie Lu, *University of Minnesota;* Ting Wang, *Pennsylvania State University*

Token-Level Fuzzing 2795
Christopher Salls, *UC Santa Barbara;* Chani Jindal, *Microsoft;* Jake Corina, *Seaside Security;* Christopher Kruegel and Giovanni Vigna, *UC Santa Barbara*

APICRAFT: Fuzz Driver Generation for Closed-source SDK Libraries 2811
Cen Zhang, *Nanyang Technological University;* Xingwei Lin, *Ant Group;* Yuekang Li, *Nanyang Technological University;* Yinxing Xue, *University of Science and Technology of China;* Jundong Xie, *Ant Group;* Hongxu Chen, *Nanyang Technological University;* Xinlei Ying and Jiashui Wang, *Ant Group;* Yang Liu, *Nanyang Technological University*

The Use of Likely Invariants as Feedback for Fuzzers 2829
Andrea Fioraldi, *EURECOM;* Daniele Cono D'Elia, *Sapienza University of Rome;* Davide Balzarotti, *EURECOM*

ICSFuzz: Manipulating I/Os and Repurposing Binary Code to Enable Instrumented Fuzzing in ICS Control Applications 2847
Dimitrios Tychalas, *NYU Tandon School of Engineering;* Hadjer Benkraouda and Michail Maniatakos, *New York University Abu Dhabi*

Web Security 2

Prime+Probe 1, JavaScript 0: Overcoming Browser-based Side-Channel Defenses 2863
Anatoly Shusterman, *Ben-Gurion University of the Negev;* Ayush Agarwal, *University of Michigan;* Sioli O'Connell, *University of Adelaide;* Daniel Genkin, *University of Michigan;* Yossi Oren, *Ben-Gurion University of the Negev;* Yuval Yarom, *University of Adelaide and Data61*

Saphire: Sandboxing PHP Applications with Tailored System Call Allowlists 2881
Alexander Bulekov, Rasoul Jahanshahi, and Manuel Egele, *Boston University*

SandTrap: Securing JavaScript-driven Trigger-Action Platforms 2899
Mohammad M. Ahmadpanah, *Chalmers University of Technology;* Daniel Hedin, *Chalmers University of Technology and Mälardalen University;* Musard Balliu, *KTH Royal Institute of Technology;* Lars Eric Olsson and Andrei Sabelfeld, *Chalmers University of Technology*

Can I Take Your Subdomain? Exploring Same-Site Attacks in the Modern Web 2917
Marco Squarcina, Mauro Tempesta, and Lorenzo Veronese, *TU Wien;* Stefano Calzavara, *Università Ca' Foscari Venezia & OWASP;* Matteo Maffei, *TU Wien*

U Can't Debug This: Detecting JavaScript Anti-Debugging Techniques in the Wild 2935
Marius Musch and Martin Johns, *TU Braunschweig*

Abusing Hidden Properties to Attack the Node.js Ecosystem 2951
Feng Xiao, *Georgia Tech;* Jianwei Huang, *Texas A&M University;* Yichang Xiong, *Independent Researcher;* Guangliang Yang, *Georgia Tech;* Hong Hu, *Penn State University;* Guofei Gu, *Texas A&M University;* Wenke Lee, *Georgia Tech*

Friday, August 13

Forensics and Diagnostics for Security and Voting

mID: Tracing Screen Photos via Moiré Patterns 2969
Yushi Cheng, Xiaoyu Ji, Lixu Wang, and Qi Pang, *Zhejiang University;* Yi-Chao Chen, *Shanghai Jiao Tong University;* Wenyuan Xu, *Zhejiang University*

SEAL: Storage-efficient Causality Analysis on Enterprise Logs with Query-friendly Compression 2987
Peng Fei, Zhou Li, and Zhiying Wang, *University of California, Irvine;* Xiao Yu, *NEC Laboratories America, Inc.;* Ding Li, *Peking University;* Kangkook Jee, *University of Texas at Dallas*

ATLAS: A Sequence-based Learning Approach for Attack Investigation 3005
Abdulellah Alsaheel and Yuhong Nan, *Purdue University;* Shiqing Ma, *Rutgers University;* Le Yu, Gregory Walkup, Z. Berkay Celik, Xiangyu Zhang, and Dongyan Xu, *Purdue University*

ELISE: A Storage Efficient Logging System Powered by Redundancy Reduction and Representation Learning . . . 3023
Hailun Ding, Shenao Yan, Juan Zhai, and Shiqing Ma, *Rutgers University*

V0Finder: Discovering the Correct Origin of Publicly Reported Software Vulnerabilities 3041
Seunghoon Woo, Dongwook Lee, Sunghan Park, and Heejo Lee, *Korea University;* Sven Dietrich, *City University of New York*

MINERVA– An Efficient Risk-Limiting Ballot Polling Audit 3059
Filip Zagórski, *Wroclaw University of Science and Technology;* Grant McClearn and Sarah Morin, *The George Washington University;* Neal McBurnett; Poorvi L. Vora, *The George Washington University*

Security Analysis of the Democracy Live Online Voting System 3077
Michael Specter, *MIT;* J. Alex Halderman, *University of Michigan*

Internet and Network Security

Hopper: Modeling and Detecting Lateral Movement 3093
Grant Ho, *UC San Diego, UC Berkeley, and Dropbox;* Mayank Dhiman, *Dropbox;* Devdatta Akhawe, *Figma, Inc.;* Vern Paxson, *UC Berkeley and International Computer Science Institute;* Stefan Savage and Geoffrey M. Voelker, *UC San Diego;* David Wagner, *UC Berkeley*

LZR: Identifying Unexpected Internet Services 3111
Liz Izhikevich, *Stanford University;* Renata Teixeira, *Inria;* Zakir Durumeric, *Stanford University*

Blind In/On-Path Attacks and Applications to VPNs 3129
William J. Tolley and Beau Kujath, *Breakpointing Bad/Arizona State University;* Mohammad Taha Khan, *Washington and Lee University;* Narseo Vallina-Rodriguez, *IMDEA Networks Institute/ICSI;* Jedidiah R. Crandall, *Breakpointing Bad/ Arizona State University*

The *Hijackers* Guide To The Galaxy: *Off-Path* Taking Over Internet Resources 3147
Tianxiang Dai, *Fraunhofer Institute for Secure Information Technology SIT;* Philipp Jeitner, *Fraunhofer Institute for Secure Information Technology SIT, Technical University of Darmstadt;* Haya Shulman, *Fraunhofer Institute for Secure Information Technology SIT;* Michael Waidner, *Fraunhofer Institute for Secure Information Technology SIT, Technical University of Darmstadt*

Injection Attacks Reloaded: Tunnelling Malicious Payloads over DNS 3165
Philipp Jeitner, *TU Darmstadt;* Haya Shulman, *Fraunhofer SIT*

Causal Analysis for Software-Defined Networking Attacks. 3183
Benjamin E. Ujcich, *Georgetown University;* Samuel Jero and Richard Skowyra, *MIT Lincoln Laboratory;* Adam Bates, *University of Illinois at Urbana-Champaign;* William H. Sanders, *Carnegie Mellon University;* Hamed Okhravi, *MIT Lincoln Laboratory*

Attacks

Weak Links in Authentication Chains: A Large-scale Analysis of Email Sender Spoofing Attacks 3201
Kaiwen Shen, Chuhan Wang, and Minglei Guo, *Tsinghua University;* Xiaofeng Zheng, *Tsinghua University and Qi An Xin Technology Research Institute;* Chaoyi Lu and Baojun Liu, *Tsinghua University;* Yuxuan Zhao, *North China Institute of Computing Technology;* Shuang Hao, *University of Texas at Dallas;* Haixin Duan, *Tsinghua University; Qi An Xin Technology Research Institute;* Qingfeng Pan, *Coremail Technology Co. Ltd;* Min Yang, *Fudan University*

Automated Discovery of Denial-of-Service Vulnerabilities in Connected Vehicle Protocols 3219
Shengtuo Hu, *University of Michigan;* Qi Alfred Chen, *UC Irvine;* Jiachen Sun, Yiheng Feng, Z. Morley Mao, and Henry X. Liu, *University of Michigan*

Too Good to Be Safe: Tricking Lane Detection in Autonomous Driving with Crafted Perturbations 3237
Pengfei Jing, *The Hong Kong Polytechnic University and Keen Security Lab, Tencent;* Qiyi Tang and Yuefeng Du, *Keen Security Lab, Tencent;* Lei Xue and Xiapu Luo, *The Hong Kong Polytechnic University;* Ting Wang, *Pennsylvania State University;* Sen Nie and Shi Wu, *Keen Security Lab, Tencent*

Acoustics to the Rescue: Physical Key Inference Attack Revisited 3255
Soundarya Ramesh and Rui Xiao, *National University of Singapore;* Anindya Maiti, *University of Oklahoma;* Jong Taek Lee, Harini Ramprasad, and Ananda Kumar, *National University of Singapore;* Murtuza Jadliwala, *University of Texas at San Antonio;* Jun Han, *National University of Singapore*

Messy States of Wiring: Vulnerabilities in Emerging Personal Payment Systems 3273
Jiadong Lou and Xu Yuan, *University of Louisiana at Lafayette;* Ning Zhang, *Washington University in St. Louis*

Research on the Security of Visual Reasoning CAPTCHA 3291
Yipeng Gao, Haichang Gao, Sainan Luo, Yang Zi, Shudong Zhang, Wenjie Mao, Ping Wang, and Yulong Shen, *Xidian University;* Jeff Yan, *Linköping University*

Dirty Road Can Attack: Security of Deep Learning based Automated Lane Centering under Physical-World Attack 3309
Takami Sato, Junjie Shen, and Ningfei Wang, *University of California, Irvine;* Yunhan Jia, *ByteDance;* Xue Lin, *Northeastern University;* Qi Alfred Chen, *University of California, Irvine*

Research on Surveillance and Censorship

Domain Shadowing: Leveraging Content Delivery Networks for Robust Blocking-Resistant Communications . . . 3327
Mingkui Wei, *George Mason University*

Weaponizing Middleboxes for TCP Reflected Amplification 3345
Kevin Bock, *University of Maryland;* Abdulrahman Alaraj, *University of Colorado Boulder;* Yair Fax and Kyle Hurley, *University of Maryland;* Eric Wustrow, *University of Colorado Boulder;* Dave Levin, *University of Maryland*

Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong 3363
Martin R. Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Mareková, *Royal Holloway, University of London*

How Great is the Great Firewall? Measuring China's DNS Censorship 3381
Nguyen Phong Hoang, *Stony Brook University and Citizen Lab, University of Toronto;* Arian Akhavan Niaki, *University of Massachusetts, Amherst;* Jakub Dalek, Jeffrey Knockel, and Pellaeon Lin, *Citizen Lab, University of Toronto;* Bill Marczak, *Citizen Lab, University of Toronto, and University of California, Berkeley;* Masashi Crete-Nishihata, *Citizen Lab, University of Toronto;* Phillipa Gill, *University of Massachusetts, Amherst;* Michalis Polychronakis, *Stony Brook University*

Balboa: Bobbing and Weaving around Network Censorship. 3399
Marc B. Rosen, James Parker, and Alex J. Malozemoff, *Galois, Inc.*

Once is Never Enough: Foundations for Sound Statistical Inference in Tor Network Experimentation. 3415
Rob Jansen, *U.S. Naval Research Laboratory;* Justin Tracey and Ian Goldberg, *University of Waterloo*

Rollercoaster: An Efficient Group-Multicast Scheme for Mix Networks 3433
Daniel Hugenroth, Martin Kleppmann, and Alastair R. Beresford, *University of Cambridge*

Malware and Program Analysis 1

Obfuscation-Resilient Executable Payload Extraction From Packed Malware 3451
Binlin Cheng, *Hubei Normal University & Wuhan University;* Jiang Ming, Erika A Leal, and Haotian Zhang, *The University of Texas at Arlington;* Jianming Fu and Guojun Peng, *Wuhan University;* Jean-Yves Marion, *Université de Lorraine, CNRS, LORIA*

DeepReflect: Discovering Malicious Functionality through Binary Reconstruction. 3469
Evan Downing, *Georgia Institute of Technology;* Yisroel Mirsky, *Georgia Institute of Technology & Ben-Gurion University;* Kyuhong Park and Wenke Lee, *Georgia Institute of Technology*

When Malware Changed Its Mind: An Empirical Study of Variable Program Behaviors in the Real World 3487
Erin Avllazagaj, *University of Maryland, College Park;* Ziyun Zhu, *Facebook;* Leyla Bilge, *NortonLifeLock Research Group;* Davide Balzarotti, *EURECOM;* Tudor Dumitras, *University of Maryland, College Park*

The Circle Of Life: A Large-Scale Study of The IoT Malware Lifecycle 3505
Omar Alrawi, Charles Lever, and Kevin Valakuzhy, *Georgia Institute of Technology;* Ryan Court and Kevin Snow, *Zero Point Dynamics;* Fabian Monrose, *University of North Carolina at Chapel Hill;* Manos Antonakakis, *Georgia Institute of Technology*

Forecasting Malware Capabilities From Cyber Attack Memory Images. 3523
Omar Alrawi, Moses Ike, Matthew Pruett, Ranjita Pai Kasturi, Srimanta Barua, Taleb Hirani, Brennan Hill, and Brendan Saltaformaggio, *Georgia Institute of Technology*

YarIx: Scalable YARA-based Malware Intelligence. 3541
Michael Brengel and Christian Rossow, *CISPA Helmholtz Center for Information Security*

Constraint-guided Directed Greybox Fuzzing. 3559
Gwangmu Lee, *Seoul National University;* Woochul Shim, *Samsung Research;* Byoungyoung Lee, *Seoul National University*

Mobile System Security and Privacy

PrivateDrop: Practical Privacy-Preserving Authentication for Apple AirDrop 3577
Alexander Heinrich, Matthias Hollick, Thomas Schneider, Milan Stute, and Christian Weinert, *TU Darmstadt*

Privacy-Preserving and Standard-Compatible AKA Protocol for 5G 3595
Yuchen Wang, *TCA of State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences & Alibaba Group;* Zhenfeng Zhang, *TCA of State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences;* Yongquan Xie, *Commercial Cryptography Testing Center of State Cryptography Administration*

SEApp: Bringing Mandatory Access Control to Android Apps 3613
Matthew Rossi, Dario Facchinetti, and Enrico Bacis, *Università degli Studi di Bergamo;* Marco Rosa, *SAP Security Research;* Stefano Paraboschi, *Università degli Studi di Bergamo*

A11y and Privacy don't have to be mutually exclusive: Constraining Accessibility Service Misuse on Android . . . 3631
Jie Huang, Michael Backes, and Sven Bugiel, *CISPA Helmholtz Center for Information Security*

An Investigation of the Android Kernel Patch Ecosystem 3649
Zheng Zhang, *UC RIverside;* Hang Zhang and Zhiyun Qian, *UC Riverside;* Billy Lau, *Google Inc.*

Share First, Ask Later (or Never?) Studying Violations of GDPR's Explicit Consent in Android Apps 3667
Trung Tin Nguyen, *CISPA Helmholtz Center for Information Security; Saarbrücken Graduate School of Computer Science, Saarland University;* Michael Backes, Ninja Marnau, and Ben Stock, *CISPA Helmholtz Center for Information Security*

DEFInit: An Analysis of Exposed Android Init Routines 3685
Yuede Ji, *University of North Texas;* Mohamed Elsabagh, Ryan Johnson, and Angelos Stavrou, *Kryptowire*

Phishing and the Malicious Web

Scalable Detection of Promotional Website Defacements in Black Hat SEO Campaigns 3703
Ronghai Yang, *Sangfor Technologies Inc.;* Xianbo Wang, *The Chinese University of Hong Kong;* Cheng Chi, Dawei Wang, Jiawei He, and Siming Pang, *Sangfor Technologies Inc.;* Wing Cheong Lau, *The Chinese University of Hong Kong*

Compromised or Attacker-Owned: A Large Scale Classification and Study of Hosting Domains of Malicious URLs. 3721
Ravindu De Silva, *SCoRe Lab and Qatar Computing Research Institute;* Mohamed Nabeel, *Qatar Computing Research Institute;* Charith Elvitigala, *SCoRe Lab;* Issa Khalil and Ting Yu, *Qatar Computing Research Institute;* Chamath Keppitiyagama, *University of Colombo School of Computing*

Assessing Browser-level Defense against IDN-based Phishing. 3739
Hang Hu, *Virginia Tech;* Steve T.K. Jan, *University of Illinois at Urbana-Champaign/Virginia Tech;* Yang Wang and Gang Wang, *University of Illinois at Urbana-Champaign*

Catching Phishers By Their Bait: Investigating the Dutch Phishing Landscape through Phishing Kit Detection . 3757
Hugo Bijmans, Tim Booij, and Anneke Schwedersky, *Netherlands Organisation for Applied Scientific Research (TNO);* Aria Nedgabat, *Eindhoven University of Technology;* Rolf van Wegberg, *Delft University of Technology*

PhishPrint: Evading Phishing Detection Crawlers by Prior Profiling 3775
Bhupendra Acharya and Phani Vadrevu, *UNO Cyber Center, University of New Orleans*

Phishpedia: A Hybrid Deep Learning Based Approach to Visually Identify Phishing Webpages. 3793
Yun Lin and Ruofan Liu, *National University of Singapore;* Dinil Mon Divakaran, *Trustwave;* Jun Yang Ng and Qing Zhou Chan, *National University of Singapore;* Yiwen Lu, Yuxuan Si, and Fan Zhang, *Zhejiang University;* Jin Song Dong, *National University of Singapore*

Is Real-time Phishing Eliminated with FIDO? Social Engineering Downgrade Attacks against FIDO Protocols . 3811
Enis Ulqinaku, *ETH Zürich;* Hala Assal, AbdelRahman Abdou, and Sonia Chiasson, *Carleton University;* Srdjan Capkun, *ETH Zürich*

DDOS; Wireless Security

Jaqen: A High-Performance Switch-Native Approach for Detecting and Mitigating Volumetric DDoS Attacks with Programmable Switches 3829
Zaoxing Liu, *Boston University;* Hun Namkung, *Carnegie Mellon University;* Georgios Nikolaidis, Jeongkeun Lee, and Changhoon Kim, *Intel, Barefoot Switch Division;* Xin Jin, *Peking University;* Vladimir Braverman, *Johns Hopkins University;* Minlan Yu, *Harvard University;* Vyas Sekar, *Carnegie Mellon University*

ReDoSHunter: A Combined Static and Dynamic Approach for Regular Expression DoS Detection 3847
Yeting Li and Zixuan Chen, *SKLCS, ISCAS, UCAS;* Jialun Cao, *HKUST;* Zhiwu Xu, *Shenzhen University;* Qiancheng Peng, *SKLCS, ISCAS, UCAS;* Haiming Chen, *SKLCS, ISCAS;* Liyuan Chen, *Tencent;* Shing-Chi Cheung, *HKUST*

Ripple: A Programmable, Decentralized Link-Flooding Defense Against Adaptive Adversaries 3865
Jiarong Xing, Wenqing Wu, and Ang Chen, *Rice University*

Accurately Measuring Global Risk of Amplification Attacks using AmpMap 3881
Soo-Jin Moon, Yucheng Yin, and Rahul Anand Sharma, *Carnegie Mellon University;* Yifei Yuan, *Alibaba Group;* Jonathan M. Spring, *CERT/CC, SEI, Carnegie Mellon University;* Vyas Sekar, *Carnegie Mellon University*

A Stealthy Location Identification Attack Exploiting Carrier Aggregation in Cellular Networks 3899
Nitya Lakshmanan and Nishant Budhdev, *National University of Singapore;* Min Suk Kang, *KAIST;* Mun Choon Chan and Jun Han, *National University of Singapore*

Disrupting *Continuity* of Apple's Wireless Ecosystem Security: New Tracking, DoS, and MitM Attacks on iOS and macOS Through Bluetooth Low Energy, AWDL, and Wi-Fi 3917
Milan Stute, Alexander Heinrich, Jannik Lorenz, and Matthias Hollick, *Technical University of Darmstadt*

Stars Can Tell: A Robust Method to Defend against GPS Spoofing Attacks using Off-the-shelf Chipset 3935
Shinan Liu, *University of Chicago;* Xiang Cheng and Hanchao Yang, *Virginia Tech;* Yuanchao Shu, *Microsoft Research;* Xiaoran Weng, *University of Electronic Science and Technology of China;* Ping Guo, *City University of Hong Kong;* Kexiong (Curtis) Zeng, *Facebook;* Gang Wang, *University of Illinois at Urbana-Champaign;* Yaling Yang, *Virginia Tech*

Cryptography and the Cloud

Formally Verified Memory Protection for a Commodity Multiprocessor Hypervisor 3953
Shih-Wei Li, Xupeng Li, Ronghui Gu, Jason Nieh, and John Zhuang Hui, *Columbia University*

Automatic Policy Generation for Inter-Service Access Control of Microservices 3971
Xing Li, *Zhejiang University;* Yan Chen, *Northwestern University;* Zhiqiang Lin, *The Ohio State University;* Xiao Wang and Jim Hao Chen, *Northwestern University*

CLARION: Sound and Clear Provenance Tracking for Microservice Deployments 3989
Xutong Chen, *Northwestern University;* Hassaan Irshad, *SRI International;* Yan Chen, *Northwestern University;* Ashish Gehani and Vinod Yegneswaran, *SRI International*

Virtual Secure Platform: A Five-Stage Pipeline Processor over TFHE 4007
Kotaro Matsuoka, Ryotaro Banno, Naoki Matsumoto, Takashi Sato, and Song Bian, *Kyoto University*

Searching Encrypted Data with Size-Locked Indexes 4025
Min Xu, *University of Chicago;* Armin Namavari, *Cornell University;* David Cash, *University of Chicago;* Thomas Ristenpart, *Cornell Tech*

Blitz: Secure Multi-Hop Payments Without Two-Phase Commits. 4043
Lukas Aumayr, *TU Wien;* Pedro Moreno-Sanchez, *IMDEA Software Institute;* Aniket Kate, *Purdue University;* Matteo Maffei, *TU Wien*

Reducing HSM Reliance in Payments through Proxy Re-Encryption 4061
Sivanarayana Gaddam, *Visa;* Atul Luykx, *Security Engineering Research, Google;* Rohit Sinha, *Swirlds Inc.;* Gaven Watson, *Visa Research*

Measurements of Fraud, Malware, Spam, and Other Abuse

Risky Business? Investigating the Security Practices of Vendors on an Online Anonymous Market using Ground-Truth Data 4079
Jochem van de Laarschot and Rolf van Wegberg, *Delft University of Technology*

Deep Entity Classification: Abusive Account Detection for Online Social Networks 4097
Teng Xu, Gerard Goossen, Huseyin Kerem Cevahir, Sara Khodeir, and Yingyezhe Jin, *Facebook, Inc;* Frank Li, *Facebook, Inc, and Georgia Institute of Technology;* Shawn Shan, *Facebook, Inc, and University of Chicago;* Sagar Patel and David Freeman, *Facebook, Inc;* Paul Pearce, *Facebook, Inc, and Georgia Institute of Technology*

SocialHEISTing: Understanding Stolen Facebook Accounts. 4115
Jeremiah Onaolapo, *University of Vermont;* Nektarios Leontiadis and Despoina Magka, *Facebook;* Gianluca Stringhini, *Boston University*

Understanding Malicious Cross-library Data Harvesting on Android 4133
Jice Wang, *National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences; Indiana University Bloomington;* Yue Xiao and Xueqiang Wang, *Indiana University Bloomington;* Yuhong Nan, *Purdue University;* Luyi Xing and Xiaojing Liao, *Indiana University Bloomington;* JinWei Dong, *School of Cyber Engineering, Xidian University;* Nicolas Serrano, *Indiana University, Bloomington;* Haoran Lu and XiaoFeng Wang, *Indiana University Bloomington;* Yuqing Zhang, *National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences; School of Cyber Engineering, Xidian University; School of Computer Science and Cyberspace Security, Hainan University*

Swiped: Analyzing Ground-truth Data of a Marketplace for Stolen Debit and Credit Cards 4151
Maxwell Aliapoulios, Cameron Ballard, Rasika Bhalerao, Tobias Lauinger, and Damon McCoy, *New York University*

Having Your Cake and Eating It: An Analysis of Concession-Abuse-as-a-Service 4169
Zhibo Sun, Adam Oest, and Penghui Zhang, *Arizona State University;* Carlos Rubio-Medrano, *Texas A&M University - Corpus Christi;* Tiffany Bao and Ruoyu Wang, *Arizona State University;* Ziming Zhao, *Rochester Institute of Technology;* Yan Shoshitaishvili and Adam Doupé, *Arizona State University;* Gail-Joon Ahn, *Arizona State University and Samsung Research*

IoT; Specialty Networking

Capture: Centralized Library Management for Heterogeneous IoT Devices. 4187
Han Zhang, Abhijith Anilkumar, Matt Fredrikson, and Yuvraj Agarwal, *Carnegie Mellon University*

MPInspector: A Systematic and Automatic Approach for Evaluating the Security of IoT Messaging Protocols . . . 4205
Qinying Wang, *Zhejiang University;* Shouling Ji, *Zhejiang University; Binjiang Institute of Zhejiang University;* Yuan Tian, *University of Virginia;* Xuhong Zhang, *Zhejiang University; Binjiang Institute of Zhejiang University;* Binbin Zhao, *Georgia Institute of Technology;* Yuhong Kan and Zhaowei Lin, *Zhejiang University;* Changting Lin and Shuiguang Deng, *Zhejiang University; Binjiang Institute of Zhejiang University;* Alex X. Liu, *Ant Group;* Raheem Beyah, *Georgia Institute of Technology*

HAWatcher: Semantics-Aware Anomaly Detection for Appified Smart Homes 4223
Chenglong Fu, *Temple University;* Qiang Zeng, *University of South Carolina;* Xiaojiang Du, *Temple University*

Exposing New Vulnerabilities of Error Handling Mechanism in CAN 4241
Khaled Serag and Rohit Bhatia, *Purdue University;* Vireshwar Kumar, *Indian Institute of Technology Delhi;* Z. Berkay Celik and Dongyan Xu, *Purdue University*

CANARY - a reactive defense mechanism for Controller Area Networks based on Active RelaYs 4259
Bogdan Groza, Lucian Popa, and Pal-Stefan Murvay, *Universitatea Politehnica Timisoara;* Yuval Elovici and Asaf Shabtai, *Ben-Gurion University of the Negev*

ReDMArk: Bypassing RDMA Security Mechanisms 4277
Benjamin Rothenberger, Konstantin Taranov, Adrian Perrig, and Torsten Hoefler, *ETH Zurich*

TLS

ALPACA: Application Layer Protocol Confusion - Analyzing and Mitigating Cracks in TLS Authentication 4293
Marcus Brinkmann, *Ruhr University Bochum;* Christian Dresen, *Münster University of Applied Sciences;* Robert Merget, *Ruhr University Bochum;* Damian Poddebniak, *Münster University of Applied Sciences;* Jens Müller, *Ruhr University Bochum;* Juraj Somorovsky, *Paderborn University;* Jörg Schwenk, *Ruhr University Bochum;* Sebastian Schinzel, *Münster University of Applied Sciences*

Experiences Deploying Multi-Vantage-Point Domain Validation at Let's Encrypt 4311
Henry Birge-Lee and Liang Wang, *Princeton University;* Daniel McCarney, *Square Inc.;* Roland Shoemaker, *unaffiliated;* Jennifer Rexford and Prateek Mittal, *Princeton University*

SiamHAN: IPv6 Address Correlation Attacks on TLS Encrypted Traffic via Siamese Heterogeneous Graph Attention Network. 4329
Tianyu Cui, Gaopeng Gou, Gang Xiong, Zhen Li, Mingxin Cui, and Chang Liu, *Institute of Information Engineering, Chinese Academy of Sciences, and School of Cyber Security, University of Chinese Academy of Sciences*

Why Eve and Mallory Still Love Android: Revisiting TLS (In)Security in Android Applications 4347
Marten Oltrogge, *CISPA Helmholtz Center for Information Security;* Nicolas Huaman, Sabrina Amft, and Yasemin Acar, *Leibniz University Hannover;* Michael Backes, *CISPA Helmholtz Center for Information Security;* Sascha Fahl, *Leibniz University Hannover*

Why TLS is better without STARTTLS: A Security Analysis of STARTTLS in the Email Context 4365
Damian Poddebniak and Fabian Ising, *Münster University of Applied Sciences;* Hanno Böck, *Independent Researcher;* Sebastian Schinzel, *Münster University of Applied Sciences*

What's in a Name? Exploring CA Certificate Control 4383
Zane Ma and Joshua Mason, *University of Illinois at Urbana-Champaign;* Manos Antonakakis, *Georgia Institute of Technology;* Zakir Durumeric, *Stanford University;* Michael Bailey, *University of Illinois at Urbana-Champaign*