

27th USENIX Security Symposium 2018 (USENIX Security'18)

Baltimore, Maryland, USA
15 – 17 August 2018

Volume 1 of 3

ISBN: 978-1-7138-0409-3

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© (2018) by Usenix Association
All rights reserved.

Printed with permission by Curran Associates, Inc. (2020)

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

USENIX Security '18:
27th USENIX Security Symposium
August 15–17, 2018
Baltimore, MD, USA

Security Impacting the Physical World

Fear the Reaper: Characterization and Fast Detection of Card Skimmers1
Nolen Scaife, Christian Peeters, and Patrick Traynor, *University of Florida*

BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid15
Saleh Soltan, Prateek Mittal, and H. Vincent Poor, *Princeton University*

Skill Squatting Attacks on Amazon Alexa33
Deepak Kumar, Riccardo Paccagnella, Paul Murley, Eric Hennenfent, Joshua Mason, Adam Bates, and Michael Bailey, *University of Illinois, Urbana-Champaign*

CommanderSong: A Systematic Approach for Practical Adversarial Voice Recognition.49
Xuejing Yuan, *SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, School of Cyber Security, University of Chinese Academy of Sciences*; Yuxuan Chen, *Florida Institute of Technology*; Yue Zhao, *SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, School of Cyber Security, University of Chinese Academy of Sciences*; Yunhui Long, *University of Illinois at Urbana-Champaign*; Xiaokang Liu and Kai Chen, *SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, School of Cyber Security, University of Chinese Academy of Sciences*; Shengzhi Zhang, *Florida Institute of Technology, Department of Computer Science, Metropolitan College, Boston University, USA*; Heqing Huang, *unaffiliated*; Xiaofeng Wang, *Indiana University Bloomington*; Carl A. Gunter, *University of Illinois at Urbana-Champaign*

Memory Defenses

ACES: Automatic Compartments for Embedded Systems.65
Abraham A Clements, *Purdue University and Sandia National Labs*; Naif Saleh Almakhdhub, Saurabh Bagchi, and Mathias Payer, *Purdue University*

IMIX: In-Process Memory Isolation EXTension83
Tommaso Frassetto, Patrick Jauernig, Christopher Liebchen, and Ahmad-Reza Sadeghi, *Technische Universität Darmstadt*

HEAPHOPPER: Bringing Bounded Model Checking to Heap Implementation Security99
Moritz Eckert, *University of California, Santa Barbara*; Antonio Bianchi, *University of California, Santa Barbara and The University of Iowa*; Ruoyu Wang, *University of California, Santa Barbara and Arizona State University*; Yan Shoshitaishvili, *Arizona State University*; Christopher Kruegel and Giovanni Vigna, *University of California, Santa Barbara*

GUARDER: A Tunable Secure Allocator117
Sam Silvestro, Hongyu Liu, and Tianyi Liu, *University of Texas at San Antonio*; Zhiqiang Lin, *Ohio State University*; Tongping Liu, *University of Texas at San Antonio*

Censorship and Web Privacy

Fp-Scanner: The Privacy Implications of Browser Fingerprint Inconsistencies135
Antoine Vastel, *Univ. Lille / Inria / Inria*; Pierre Laperdrix, *Stony Brook University*; Walter Rudametkin, *Univ. Lille / Inria / Inria*; Romain Rouvoy, *Univ. Lille / Inria / IUF*

Who Left Open the Cookie Jar? A Comprehensive Evaluation of Third-Party Cookie Policies151
Gertjan Franken, Tom Van Goethem, and Wouter Joosen, *imec-DistriNet, KU Leuven*

Effective Detection of Multimedia Protocol Tunneling using Machine Learning169
Diogo Barradas, Nuno Santos, and Luís Rodrigues, *INESC-ID, Instituto Superior Técnico, Universidade de Lisboa*

Quack: Scalable Remote Measurement of Application-Layer Censorship187
Benjamin VanderSloot, Allison McDonald, Will Scott, J. Alex Halderman, and Roya Ensafi, *University of Michigan*

Understanding How Humans Authenticate

Better managed than memorized? Studying the Impact of Managers on Password Strength and Reuse . . .203
Sanam Ghorbani Lyastani, *CISPA, Saarland University*; Michael Schilling, *Saarland University*; Sascha Fahl, *Ruhr-University Bochum*; Michael Backes and Sven Bugiel, *CISPA Helmholtz Center i.G.*

Forgetting of Passwords: Ecological Theory and Data221
Xianyi Gao, Yulong Yang, Can Liu, Christos Mitropoulos, and Janne Lindqvist, *Rutgers University*;
Antti Oulasvirta, *Aalto University*

The Rewards and Costs of Stronger Passwords in a University: Linking Password Lifetime to Strength 239
Ingolf Becker, Simon Parkin, and M. Angela Sasse, *University College London*

Rethinking Access Control and Authentication for the Home Internet of Things (IoT)255
Weijia He, *University of Chicago*; Maximilian Golla, *Ruhr-University Bochum*; Roshni Padhi and Jordan Ofek, *University of Chicago*; Markus Dürmuth, *Ruhr-University Bochum*; Earlene Fernandes, *University of Washington*;
Blase Ur, *University of Chicago*

Vulnerability Discovery

ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem273
Dave (Jing) Tian, Grant Hernandez, Joseph I. Choi, Vanessa Frost, Christie Ruales, and Patrick Traynor, *University of Florida*; Hayawardh Vijayakumar and Lee Harrison, *Samsung Research America*; Amir Rahmati, *Samsung Research America and Stony Brook University*; Michael Grace, *Samsung Research America*; Kevin R. B. Butler, *University of Florida*

Charm: Facilitating Dynamic Analysis of Device Drivers of Mobile Systems291
Seyed Mohammadjavad Seyed Talebi and Hamid Tavakoli, *UC Irvine*; Hang Zhang and Zheng Zhang, *UC Riverside*; Ardalan Amiri Sani, *UC Irvine*; Zhiyun Qian, *UC Riverside*

Inception: System-Wide Security Testing of Real-World Embedded Systems Software309
Nassim Corteggiani, *EURECOM, Maxim Integrated*; Giovanni Camurati and Aurélien Francillon, *EURECOM*

Acquisitional Rule-based Engine for Discovering Internet-of-Thing Devices327
Xuan Feng, *Beijing Key Laboratory of IOT Information Security Technology, IIE, CAS, China, and School of Cyber Security, University of Chinese Academy of Sciences, China*; Qiang Li, *School of Computer and Information Technology, Beijing Jiaotong University, China*; Haining Wang, *Department of Electrical and Computer Engineering, University of Delaware, USA*; Limin Sun, *Beijing Key Laboratory of IOT Information Security Technology, IIE, CAS, China, and School of Cyber Security, University of Chinese Academy of Sciences, China*

Web Applications

A Sense of Time for JavaScript and Node.js: First-Class Timeouts as a Cure for Event Handler Poisoning. . .343
James C. Davis, Eric R. Williamson, and Dongyoon Lee, *Virginia Tech*

Freezing the Web: A Study of ReDoS Vulnerabilities in JavaScript-based Web Servers361
Cristian-Alexandru Staicu and Michael Pradel, *TU Darmstadt*

NAVEX: Precise and Scalable Exploit Generation for Dynamic Web Applications377
Abeer Alhuzali, Rigel Gjomemo, Birhanu Eshete, and V.N. Venkatakrisnan, *University of Illinois at Chicago*

Rampart: Protecting Web Applications from CPU-Exhaustion Denial-of-Service Attacks393
Wei Meng, *Chinese University of Hong Kong*; Chenxiong Qian, *Georgia Institute of Technology*; Shuang Hao, *University of Texas at Dallas*; Kevin Borgolte, Giovanni Vigna, and Christopher Kruegel, *University of California, Santa Barbara*; Wenke Lee, *Georgia Institute of Technology*

Anonymity

How Do Tor Users Interact With Onion Services?411
Philipp Winter, Anne Edmundson, and Laura M. Roberts, *Princeton University*; Agnieszka Dutkowska-Żuk, *Independent*; Marshini Chetty and Nick Feamster, *Princeton University*

Towards Predicting Efficient and Anonymous Tor Circuits429
Armon Barton, Mohsen Imani, and Jiang Ming, *University of Texas at Arlington*; Matthew Wright, *Rochester Institute of Technology*

BurnBox: Self-Revocable Encryption in a World Of Compelled Access445
Nirvan Tyagi, *Cornell University*; Muhammad Haris Mughees, *UIUC*; Thomas Ristenpart and Ian Miers, *Cornell Tech*

An Empirical Analysis of Anonymity in Zcash463
George Kappos, Haaron Yousaf, Mary Maller, and Sarah Meiklejohn, *University College London*

Privacy in a Digital World

Unveiling and Quantifying Facebook Exploitation of Sensitive Personal Data for Advertising Purposes . . .479
José González Cabañas, Ángel Cuevas, and Rubén Cuevas, *Department of Telematic Engineering, Universidad Carlos III de Madrid*

Analysis of Privacy Protections in Fitness Tracking Social Networks -or- You can run, but can you hide? . . . 497
Wajih Ul Hassan, Saad Hussain, and Adam Bates, *University Of Illinois Urbana-Champaign*

AttriGuard: A Practical Defense Against Attribute Inference Attacks via Adversarial Machine Learning 513
Jinyuan Jia and Neil Zhenqiang Gong, *Iowa State University*

Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning531
Hamza Harkous, *École Polytechnique Fédérale de Lausanne (EPFL)*; Kassem Fawaz, *University of Wisconsin-Madison*; Rémi Leuret, *École Polytechnique Fédérale de Lausanne (EPFL)*; Florian Schaub and Kang G. Shin, *University of Michigan*; Karl Aberer, *École Polytechnique Fédérale de Lausanne (EPFL)*

Attacks on Crypto & Crypto Libraries

Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels549
Damian Poddebniak and Christian Dresen, *Münster University of Applied Sciences*; Jens Müller, *Ruhr University Bochum*; Fabian Ising and Sebastian Schinzel, *Münster University of Applied Sciences*; Simon Friedberger, *NXP Semiconductors, Belgium*; Juraj Somorovsky and Jörg Schwenk, *Ruhr University Bochum*

The Dangers of Key Reuse: Practical Attacks on IPsec IKE567
Dennis Felsch, Martin Grothe, and Jörg Schwenk, *Ruhr-University Bochum*; Adam Czubak and Marcin Szymanek, *University of Opole*

One&Done: A Single-Decryption EM-Based Attack on OpenSSL's Constant-Time Blinded RSA585
Monjur Alam, Haider Adnan Khan, Moumita Dey, Nishith Sinha, Robert Callan, Alenka Zajic, and Milos Prvulovic, *Georgia Tech*

DATA – Differential Address Trace Analysis: Finding Address-based Side-Channels in Binaries603
Samuel Weiser, *Graz University of Technology*; Andreas Zankl, *Fraunhofer AISEC*; Raphael Spreitzer, *Graz University of Technology*; Katja Miller, *Fraunhofer AISEC*; Stefan Mangard, *Graz University of Technology*; Georg Sigl, *Fraunhofer AISEC*; *Technical University of Munich*

Enterprise Security

The Battle for New York: A Case Study of Applied Digital Threat Modeling at the Enterprise Level621
Rock Stevens, Daniel Votipka, and Elissa M. Redmiles, *University of Maryland*; Colin Ahern, *NYC Cyber Command*; Patrick Sweeney, *Wake Forest University*; Michelle L. Mazurek, *University of Maryland*

SAQL: A Stream-based Query System for Real-Time Abnormal System Behavior Detection639
Peng Gao, *Princeton University*; Xusheng Xiao, *Case Western Reserve University*; Ding Li, Zhichun Li, Kangkook Jee, Zhenyu Wu, and Chung Hwan Kim, *NEC Laboratories America, Inc.*; Sanjeev R. Kulkarni and Prateek Mittal, *Princeton University*

Zero-Knowledge

Practical Accountability of Secret Processes657
Jonathan Frankle, Sunoo Park, Daniel Shaar, Shafi Goldwasser, and Daniel Weitzner, *Massachusetts Institute of Technology*

DIZK: A Distributed Zero Knowledge Proof System675
Howard Wu, Wenting Zheng, Alessandro Chiesa, Raluca Ada Popa, and Ion Stoica, *UC Berkeley*

Network Defenses

NetHide: Secure and Practical Network Topology Obfuscation693
Roland Meier and Petar Tsankov, *ETH Zurich*; Vincent Lenders, *armasuisse*; Laurent Vanbever and Martin Vechev, *ETH Zurich*

Towards a Secure Zero-rating Framework with Three Parties711
Zhiheng Liu and Zhen Zhang, *Lehigh University*; Yinzhi Cao, *The Johns Hopkins University/Lehigh University*; Zhaohan Xi and Shihao Jing, *Lehigh University*; Humberto La Roche, *Cisco Systems*

Fuzzing and Exploit Generation

MoonShine: Optimizing OS Fuzzer Seed Selection with Trace Distillation729
Shankara Pailoor, Andrew Aday, and Suman Jana, *Columbia University*

QSYM : A Practical Concolic Execution Engine Tailored for Hybrid Fuzzing745
Insu Yun, Sangho Lee, and Meng Xu, *Georgia Institute of Technology*; Yeongjin Jang, *Oregon State University*; Taesoo Kim, *Georgia Institute of Technology*

Automatic Heap Layout Manipulation for Exploitation763
Sean Heelan, Tom Melham, and Daniel Kroening, *University of Oxford*

FUZE: Towards Facilitating Exploit Generation for Kernel Use-After-Free Vulnerabilities781
Wei Wu, *University of Chinese Academy of Sciences; Pennsylvania State University; Institute of Information Engineering, Chinese Academy of Sciences*; Yueqi Chen, Jun Xu, and Xinyu Xing, *Pennsylvania State University*; Xiaorui Gong and Wei Zou, *University of Chinese Academy of Sciences; Institute of Information Engineering, Chinese Academy of Sciences*

TLS and PKI

The Secure Socket API: TLS as an Operating System Service799
Mark O'Neill, Scott Heidbrink, Jordan Whitehead, Tanner Perdue, Luke Dickinson, Torstein Collett, Nick Bonner, Kent Seamons, and Daniel Zappala, *Brigham Young University*

Return Of Bleichenbacher's Oracle Threat (ROBOT)817
Hanno Böck, *unaffiliated*; Juraj Somorovsky, *Ruhr University Bochum, Hackmanit GmbH*; Craig Young, *Tripwire VERT*

Bamboozling Certificate Authorities with BGP833
Henry Birge-Lee, Yixin Sun, Anne Edmundson, Jennifer Rexford, and Prateek Mittal, *Princeton University*

The Broken Shield: Measuring Revocation Effectiveness in the Windows Code-Signing PKI851
Doowon Kim and Bum Jun Kwon, *University of Maryland, College Park*; Kristián Kozák, *Masaryk University, Czech Republic*; Christopher Gates, *Symantec*; Tudor Dumitras, *University of Maryland, College Park*

Vulnerability Mitigations

Debloating Software through Piece-Wise Compilation and Loading869
Anh Quach and Aravind Prakash, *Binghamton University*; Lok Yan, *Air Force Research Laboratory*

Precise and Accurate Patch Presence Test for Binaries887
Hang Zhang and Zhiyun Qian, *University of California, Riverside*

From Patching Delays to Infection Symptoms: Using Risk Profiles for an Early Discovery of Vulnerabilities Exploited in the Wild903
Chaowei Xiao and Armin Sarabi, *University of Michigan*; Yang Liu, *Harvard University / UC Santa Cruz*; Bo Li, *UIUC*; Mingyan Liu, *University of Michigan*; Tudor Dumitras, *University of Maryland, College Park*

Understanding the Reproducibility of Crowd-reported Security Vulnerabilities919
Dongliang Mu, *Nanjing University*; Alejandro Cuevas, *The Pennsylvania State University*; Limin Yang and Hang Hu, *Virginia Tech*; Xinyu Xing, *The Pennsylvania State University*; Bing Mao, *Nanjing University*; Gang Wang, *Virginia Tech*

Side Channels

Malicious Management Unit: Why Stopping Cache Attacks in Software is Harder Than You Think937
Stephan van Schaik, Cristiano Giuffrida, Herbert Bos, and Kaveh Razavi, *Vrije Universiteit Amsterdam*

Translation Leak-aside Buffer: Defeating Cache Side-channel Protections with TLB Attacks.955
Ben Gras, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida, *Vrije Universiteit*

Meltdown: Reading Kernel Memory from User Space.973
Moritz Lipp, Michael Schwarz, and Daniel Gruss, *Graz University of Technology*; Thomas Prescher and Werner Haas, *Cyberus Technology*; Anders Fogh, *G DATA Advanced Analytics*; Jann Horn, *Google Project Zero*; Stefan Mangard, *Graz University of Technology*; Paul Kocher, *Independent*; Daniel Genkin, *University of Michigan*; Yuval Yarom, *University of Adelaide and Data61*; Mike Hamburg, *Rambus, Cryptography Research Division*

FORESHADOW: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution991
Jo Van Bulck, *imec-DistriNet, KU Leuven*; Marina Minkin, *Technion*; Ofir Weisse, Daniel Genkin, and Baris Kasikci, *University of Michigan*; Frank Piessens, *imec-DistriNet, KU Leuven*; Mark Silberstein, *Technion*; Thomas F. Wenisch, *University of Michigan*; Yuval Yarom, *University of Adelaide and Data61*; Raoul Strackx, *imec-DistriNet, KU Leuven*

Cybercrime

Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets1009
Rolf van Wegberg and Samaneh Tajalizadehkhoob, *Delft University of Technology*; Kyle Soska, *Carnegie Mellon University*; Ugur Akyazi, Carlos Hernandez Ganán, and Bram Klievink, *Delft University of Technology*; Nicolas Christin, *Carnegie Mellon University*; Michel van Eeten, *Delft University of Technology*

Reading Thieves' Cant: Automatically Identifying and Understanding Dark Jargons from Cybercrime Marketplaces1027
Kan Yuan, Haoran Lu, Xiaojing Liao, and XiaoFeng Wang, *Indiana University Bloomington*

Schrödinger's RAT: Profiling the Stakeholders in the Remote Access Trojan Ecosystem.1043
Mohammad Rezaeirad, *George Mason University*; Brown Farinholt, *University of California, San Diego*; Hitesh Dharmdasani, *Informant Networks*; Paul Pearce, *University of California, Berkeley*; Kirill Levchenko, *University of California, San Diego*; Damon McCoy, *New York University*

The aftermath of a crypto-ransomware attack at a large academic institution1061
Leah Zhang-Kennedy, *University of Waterloo, Stratford Campus*; Hala Assal, Jessica Rocheleau,
Reham Mohamed, Khadija Baig, and Sonia Chiasson, *Carleton University*

Web and Network Measurement

We Still Don't Have Secure Cross-Domain Requests: an Empirical Study of CORS1079
Jianjun Chen, *Tsinghua University*; Jian Jiang, *Shope Security*; Haixin Duan, *Tsinghua University*;
Tao Wan, *Huawei Canada*; Shuo Chen, *Microsoft Research*; Vern Paxson, *UC Berkeley, ICSI*; Min Yang,
Fudan University

End-to-End Measurements of Email Spoofing Attacks1095
Hang Hu and Gang Wang, *Virginia Tech*

**Who Is Answering My Queries: Understanding and Characterizing Interception of the DNS
Resolution Path1113**
Baojun Liu, Chaoyi Lu, Haixin Duan, and Ying Liu, *Tsinghua University*; Zhou Li, *IEEE member*; Shuang Hao,
University of Texas at Dallas; Min Yang, *Fudan University*

End-Users Get Maneuvered: Empirical Analysis of Redirection Hijacking in Content Delivery Networks 1129
Shuai Hao, Yubao Zhang, and Haining Wang, *University of Delaware*; Angelos Stavrou, *George Mason University*

Malware

**SAD THUG: Structural Anomaly Detection for Transmissions of High-value Information
Using Graphics1147**
Jonathan P. Chapman, *Fraunhofer FKIE*

FANCI : Feature-based Automated NXDomain Classification and Intelligence.1165
Samuel Schuppen, *RWTH Aachen University*; Dominik Teubert, *Siemens CERT*; Patrick Herrmann and
Ulrike Meyer, *RWTH Aachen University*

An Empirical Study of Web Resource Manipulation in Real-world Mobile Applications1183
Xiaohan Zhang, Yuan Zhang, Qianqian Mo, Hao Xia, Zhemin Yang, and Min Yang, *Fudan University*;
Xiaofeng Wang, *Indiana University, Bloomington*; Long Lu, *Northeastern University*; Haixin Duan,
Tsinghua University

Fast and Service-preserving Recovery from Malware Infections Using CRIU1199
Ashton Webster, Ryan Eckenrod, and James Purtilo, *University of Maryland*

Subverting Hardware Protections

The Guard's Dilemma: Efficient Code-Reuse Attacks Against Intel SGX.1213
Andrea Biondo and Mauro Conti, *University of Padua*; Lucas Davi, *University of Duisburg-Essen*;
Tommaso Frassetto and Ahmad-Reza Sadeghi, *Technische Universität Darmstadt*

A Bad Dream: Subverting Trusted Platform Module While You Are Sleeping.1229
Seunghun Han, Wook Shin, Jun-Hyeok Park, and HyoungChun Kim, *National Security Research Institute*

More Malware

Tackling runtime-based obfuscation in Android with TIRO.1247
Michelle Y. Wong and David Lie, *University of Toronto*

Discovering Flaws in Security-Focused Static Analysis Tools for Android using Systematic Mutation1263
Richard Bonett, Kaushal Kafle, Kevin Moran, Adwait Nadkarni, and Denys Poshyvanyk, *William & Mary*

Attacks on Systems That Learn

- With Great Training Comes Great Vulnerability: Practical Attacks against Transfer Learning**1281
Bolun Wang, *UC Santa Barbara*; Yuanshun Yao, *University of Chicago*; Bimal Viswanath, *Virginia Tech*;
Haitao Zheng and Ben Y. Zhao, *University of Chicago*
- When Does Machine Learning FAIL? Generalized Transferability for Evasion and Poisoning Attacks** . . .1299
Octavian Suci, Radu Marginean, Yigitcan Kaya, Hal Daume III, and Tudor Dumitras, *University of Maryland*

Smart Contracts

- TEETHER: Gnawing at Ethereum to Automatically Exploit Smart Contracts**1317
Johannes Krupp and Christian Rossow, *CISPA, Saarland University, Saarland Informatics Campus*
- Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts**1335
Lorenz Breidenbach, *Cornell Tech, IC3, ETH Zurich*; Philip Daian, *Cornell Tech, IC3*; Florian Tramer, *Stanford*;
Ari Juels, *Cornell Tech, IC3, Jacobs Institute*
- Arbitrum: Scalable, private smart contracts**1353
Harry Kalodner, Steven Goldfeder, Xiaoqi Chen, S. Matthew Weinberg, and Edward W. Felten,
Princeton University
- Erays: Reverse Engineering Ethereum's Opaque Smart Contracts**1371
Yi Zhou, Deepak Kumar, Surya Bakshi, Joshua Mason, Andrew Miller, and Michael Bailey, *University of Illinois, Urbana-Champaign*

Executing in Untrusted Environments

- DELEGATEE: Brokered Delegation Using Trusted Execution Environments**1387
Sinisa Matetic and Moritz Schneider, *ETH Zurich*; Andrew Miller, *UIUC*; Ari Juels, *Cornell Tech*;
Srdjan Capkun, *ETH Zurich*
- Simple Password-Hardened Encryption Services**1405
Russell W. F. Lai and Christoph Egger, *Friedrich-Alexander University Erlangen-Nuremberg*; Manuel Reinert,
Saarland University; Sherman S. M. Chow, *Chinese University of Hong Kong*; Matteo Maffei, *Vienna University of Technology*; Dominique Schröder, *Friedrich-Alexander University Erlangen-Nuremberg*
- Security Namespace: Making Linux Security Frameworks Available to Containers**1423
Yuqiong Sun, *Symantec Research Labs*; David Safford, *GE Global Research*; Mimi Zohar, Dimitrios Pendarakis,
and Zhongshu Gu, *IBM Research*; Trent Jaeger, *Pennsylvania State University*
- Shielding Software From Privileged Side-Channel Attacks**1441
Xiaowan Dong, Zhuojia Shen, and John Criswell, *University of Rochester*; Alan L. Cox, *Rice University*;
Sandhya Dwarkadas, *University of Rochester*

Web Authentication

- Vetting Single Sign-On SDK Implementations via Symbolic Reasoning**1459
Ronghai Yang, *The Chinese University of Hong Kong, Sangfor Technologies Inc.*; Wing Cheong Lau,
Jiongyi Chen, and Kehuan Zhang, *The Chinese University of Hong Kong*
- O Single Sign-Off, Where Art Thou? An Empirical Analysis of Single Sign-On Account Hijacking and Session Management on the Web**1475
Mohammad Ghasemisharif, Amrutha Ramesh, Stephen Checkoway, Chris Kanich, and Jason Polakis, *University of Illinois at Chicago*
- WPSE: Fortifying Web Protocols via Browser-Side Security Monitoring**1493
Stefano Calzavara and Riccardo Focardi, *Università Ca' Foscari Venezia*; Matteo Maffei and Clara Schneidewind, *TU Wien*; Marco Squarcina and Mauro Tempesta, *Università Ca' Foscari Venezia*

Man-in-the-Machine: Exploiting III-Secured Communication Inside the Computer1511
Thanh Bui and Siddharth Prakash Rao, *Aalto University*; Markku Antikainen, *University of Helsinki*;
Viswanathan Manihatty Bojan and Tuomas Aura, *Aalto University*

Wireless Attacks

All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems.1527
Kexiong (Curtis) Zeng, *Virginia Tech*; Shinan Liu, *University of Electronic Science and Technology of China*;
Yuanchao Shu, *Microsoft Research*; Dong Wang, Haoyu Li, Yanzhi Dou, Gang Wang, and Yaling Yang,
Virginia Tech

Injected and Delivered: Fabricating Implicit Control over Actuation Systems by Spoofing Inertial Sensors. . . 1545
Yazhou Tu, *University of Louisiana at Lafayette*; Zhiqiang Lin, *Ohio State University*; Insup Lee, *University of Pennsylvania*; Xiali Hei, *University of Louisiana at Lafayette*

Modelling and Analysis of a Hierarchy of Distance Bounding Attacks1563
Tom Chothia, *Univ. of Birmingham*; Joeri de Ruiter, *Radboud University Nijmegen*; Ben Smyth, *University of Luxembourg*

Off-Path TCP Exploit: How Wireless Routers Can Jeopardize Your Secrets1581
Weiteng Chen and Zhiyun Qian, *University of California, Riverside*

Neural Networks

Formal Security Analysis of Neural Networks using Symbolic Intervals1599
Shiqi Wang, Kexin Pei, Justin Whitehouse, Junfeng Yang, and Suman Jana, *Columbia University*

Turning Your Weakness Into a Strength: Watermarking Deep Neural Networks by Backdooring1615
Yossi Adi and Carsten Baum, *Bar Ilan University*; Moustapha Cisse, *Google Inc*; Benny Pinkas and Joseph Keshet, *Bar Ilan University*

A⁴NT: Author Attribute Anonymity by Adversarial Training of Neural Machine Translation1633
Rakshith Shetty, Bernt Schiele, and Mario Fritz, *Max Planck Institute for Informatics*

GAZELLE: A Low Latency Framework for Secure Neural Network Inference1651
Chiraag Juvekar, *MIT MTL*; Vinod Vaikuntanathan, *MIT CSAIL*; Anantha Chandrakasan, *MIT MTL*

Information Tracking

FlowCog: Context-aware Semantics Extraction and Analysis of Information Flow Leaks in Android Apps1669
Xiang Pan, *Google Inc./Northwestern University*; Yinzhi Cao, *The Johns Hopkins University/Lehigh University*;
Xuechao Du and Boyuan He, *Zhejiang University*; Gan Fang, *Palo Alto Networks*; Yan Chen, *Zhejiang University/Northwestern University*

Sensitive Information Tracking in Commodity IoT1687
Z. Berkay Celik, *The Pennsylvania State University*; Leonardo Babun, Amit Kumar Sikder, and Hidayet Aksu, *Florida International University*; Gang Tan and Patrick McDaniel, *The Pennsylvania State University*;
A. Selcuk Uluagac, *Florida International University*

Enabling Refinable Cross-Host Attack Investigation with Efficient Data Flow Tagging and Tracking . . . 1705
Yang Ji, Sangho Lee, Mattia Fazzini, Joey Allen, Evan Downing, Taesoo Kim, Alessandro Orso, and Wenke Lee, *Georgia Institute of Technology*

Dependence-Preserving Data Compaction for Scalable Forensic Analysis1723
Md Nahid Hossain, Junao Wang, R. Sekar, and Scott D. Stoller, *Stony Brook University*