

23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020)

Online
14-16 October 2020

ISBN: 978-1-7138-2600-2

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© (2020) by Usenix Association
All rights reserved.

Printed with permission by Curran Associates, Inc. (2021)

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

23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020)

October 14–16, 2020

Wednesday, October 14

Attacks

SpecROP: Speculative Exploitation of ROP Chains 1
Atri Bhattacharyya and Andrés Sánchez, *EPFL*; Esmail M. Koruyeh, Nael Abu-Ghazaleh, and Chengyu Song, *UC Riverside*; Mathias Payer, *EPFL*

Never Trust Your Victim: Weaponizing Vulnerabilities in Security Scanners 17
Andrea Valenza, *University of Genova*; Gabriele Costa, *IMT School for Advanced Studies Lucca*; Alessandro Armando, *University of Genova*

Camera Fingerprinting Authentication Revisited 31
Dominik Maier, *Technische Universität Berlin*; Henrik Erb, Patrick Mullan, and Vincent Hupert, *Friedrich-Alexander-Universität Erlangen-Nürnberg*

Dynamic Program Analysis

Binary-level Directed Fuzzing for Use-After-Free Vulnerabilities 47
Manh-Dung Nguyen and Sébastien Bardin, *Univ. Paris-Saclay, CEA LIST, France*; Richard Bonichon, *Tweag I/O, France*; Roland Groz, *Univ. Grenoble Alpes, France*; Matthieu Lemerre, *Univ. Paris-Saclay, CEA LIST, France*

WearFlow: Expanding Information Flow Analysis To Companion Apps in Wear OS 63
Marcos Tileria and Jorge Blasco, *Royal Holloway, University of London*; Guillermo Suarez-Tangil, *King's College London, IMDEA Networks*

MEUZZ: Smart Seed Scheduling for Hybrid Fuzzing 77
Yaohui Chen, Mansour Ahmadi, and Reza Mirzazade farkhani, *Northeastern University*; Boyu Wang, *Stony Brook University*; Long Lu, *Northeastern University*

Web Security

Tracing and Analyzing Web Access Paths Based on User-Side Data Collection: How Do Users Reach Malicious URLs? 93
Takeshi Takahashi, *National Institute of Information and Communications Technology*; Christopher Kruegel and Giovanni Vigna, *University of California, Santa Barbara*; Katsunari Yoshioka, *Yokohama National University*; Daisuke Inoue, *National Institute of Information and Communications Technology*

What's in an Exploit? An Empirical Analysis of Reflected Server XSS Exploitation Techniques 107
Ahmet Salih Buyukkayhan, *Microsoft*; Can Gemicioğlu, *Northeastern University*; Tobias Lauinger, *New York University*; Alina Oprea, William Robertson, and Engin Kirda, *Northeastern University*

Mininode: Reducing the Attack Surface of Node.js Applications 121
Igibek Koishybayev and Alexandros Kapravelos, *North Carolina State University*

Evaluating Changes to Fake Account Verification Systems 135
Fedor Kozlov, Isabella Yuen, Jakub Kowalczyk, Daniel Bernhardt, and David Freeman, *Facebook, Inc*; Paul Pearce, *Facebook, Inc and Georgia Institute of Technology*; Ivan Ivanov, *Facebook, Inc*

Thursday, October 15

Malware

- SourceFinder: Finding Malware Source-Code from Publicly Available Repositories in GitHub**149
Md Omar Faruk Rokon, Risul Islam, Ahmad Darki, Evangelos E. Papalexakis, and Michalis Faloutsos, *UC Riverside*
- HyperLeech: Stealthy System Virtualization with Minimal Target Impact through DMA-Based Hypervisor Injection** 165
Ralph Palutke, Simon Ruderich, Matthias Wild, and Felix Freiling, *Friedrich-Alexander-Universität Erlangen*
- Effective Detection of Credential Thefts from Windows Memory: Learning Access Behaviours to Local Security Authority Subsystem Service** 181
Patrick Ah-Fat and Michael Huth, *Imperial College London*; Rob Mead, Tim Burrell, and Joshua Neil, *Microsoft*

Network & Cloud Security

- EnclavePDP: A General Framework to Verify Data Integrity in Cloud Using Intel SGX** 195
Yun He, *Institute of Information Engineering, Chinese Academy of Sciences, and School of Cyber Security, University of Chinese Academy of Sciences*; Yihua Xu, *Metropolitan College, Boston University*; Xiaoqi Jia, *Institute of Information Engineering, Chinese Academy of Sciences, and School of Cyber Security, University of Chinese Academy of Sciences*; Shengzhi Zhang, *Metropolitan College, Boston University*; Peng Liu, *Pennsylvania State University*; Shuai Chang, *Institute of Information Engineering, Chinese Academy of Sciences, and School of Cyber Security, University of Chinese Academy of Sciences*
- Robust P2P Primitives Using SGX Enclaves** 209
Yaoqi Jia, *ACM Member*; Shruti Tople, *Microsoft Research*; Tarik Moataz, *Aroki Systems*; Deli Gong, *ACM Member*; Prateek Saxena and Zhenkai Liang, *National University of Singapore*
- aBBRate: Automating BBR Attack Exploration Using a Model-Based Approach** 225
Anthony Peterson, *Northeastern University*; Samuel Jero, *Purdue University*; Endadul Hoque, *Syracuse University*; David Choffnes and Cristina Nita-Rotaru, *Northeastern University*

ML-Based Security

- Cyber Threat Intelligence Modeling Based on Heterogeneous Graph Convolutional Network** 241
Jun Zhao, *Beihang University*; Qiben Yan, *Michigan State University*; Xudong Liu, Bo Li, and Guangsheng Zuo, *Beihang University*
- Detecting Lateral Movement in Enterprise Computer Networks with Unsupervised Graph AI** 257
Benjamin Bowman, Craig Laprade, Yuede Ji, and H. Howie Huang, *Graph Computing Lab, George Washington University*
- An Object Detection based Solver for Google's Image reCAPTCHA v2** 269
Md Imran Hossen, Yazhou Tu, Md Fazle Rabby, and Md Nazmul Islam, *University of Louisiana at Lafayette*; Hui Cao, *Xi'an Jiaotong University*; Xiali Hei, *University of Louisiana at Lafayette*

Breaking ML

- Evasion Attacks against Banking Fraud Detection Systems** 285
Michele Carminati, Luca Santini, Mario Polino, and Stefano Zanero, *Politecnico di Milano*
- The Limitations of Federated Learning in Sybil Settings** 301
Clement Fung, *Carnegie Mellon University*; Chris J. M. Yoon and Ivan Beschastnikh, *University of British Columbia*
- GhostImage: Remote Perception Attacks against Camera-based Image Classification Systems**317
Yanmao Man and Ming Li, *University of Arizona*; Ryan Gerdes, *Virginia Tech*

Friday, October 16

CPS Security

PLC-Sleuth: Detecting and Localizing PLC Intrusions Using Control Invariants 333
Zeyu Yang, *Zhejiang University*; Liang He, *University of Colorado Denver*; Peng Cheng and Jiming Chen, *Zhejiang University*; David K.Y. Yau, *Singapore University of Technology and Design*; Linkang Du, *Zhejiang University*

Software-based Realtime Recovery from Sensor Attacks on Robotic Vehicles 349
Hongjun Choi and Sayali Kate, *Purdue University*; Yousra Aafer, *University of Waterloo*; Xiangyu Zhang and Dongyan Xu, *Purdue University*

SIEVE: Secure In-Vehicle Automatic Speech Recognition Systems 365
Shu Wang, *George Mason University*; Jiahao Cao, *George Mason University and Tsinghua University*; Kun Sun, *George Mason University*; Qi Li, *Tsinghua University and Beijing National Research Center for Information Science and Technology*

Firmware and Low Level Security

μ SBS: Static Binary Sanitization of Bare-metal Embedded Devices for Fault Observability 381
Majid Salehi and Danny Hughes, *imec-Distrinet, KU Leuven*; Bruno Crispo, *imec-Distrinet, KU Leuven, and Trento University, Italy*

BlueShield: Detecting Spoofing Attacks in Bluetooth Low Energy Networks 397
Jianliang Wu, Yuhong Nan, and Vireshwar Kumar, *Purdue University*; Mathias Payer, *EPFL*; Dongyan Xu, *Purdue University*

Dark Firmware: A Systematic Approach to Exploring Application Security Risks in the Presence of Untrusted Firmware 413
Duha Ibdah, Nada Lachtar, Abdulrahman Abu Elkhail, Anys Bacha, and Hafiz Malik, *University of Michigan, Dearborn*

Systems Security

A Framework for Software Diversification with ISA Heterogeneity 427
Xiaoguang Wang, SengMing Yeoh, and Robert Lyerly, *Virginia Tech*; Pierre Olivier, *The University of Manchester*; Sang-Hoon Kim, *Ajou University*; Binoy Ravindran, *Virginia Tech*

Confine: Automated System Call Policy Generation for Container Attack Surface Reduction 443
Seyedhamed Ghavamnia and Tapti Palit, *Stony Brook University*; Azzedine Benameur, *Cloudhawk.io*; Michalis Polychronakis, *Stony Brook University*

sysfilter: Automated System Call Filtering for Commodity Software 459
Nicholas DeMarinis, Kent Williams-King, Di Jin, Rodrigo Fonseca, and Vasileios P. Kemerlis, *Brown University*