

22nd International Symposium on Research in Attacks, Intrusions and Defenses 2019

Beijing, China
23-25 September 2019

ISBN: 978-1-7138-2599-9

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© (2019) 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

**RAID 2019: 22nd International Symposium on
Research in Attacks, Intrusions and Defenses**
September 23–25, 2019
Beijing, China

Software Security

- Be Sensitive and Collaborative: Analyzing Impact of Coverage Metrics in Greybox Fuzzing** 1
Jinghan Wang, *University of California, Riverside*; Yue Duan, *Cornell University*; Wei Song, Heng Yin,
and Chengyu Song, *University of California, Riverside*
- On Design Inference from Binaries Compiled using Modern C++ Defenses**17
Rukayat Ayomide Erinfolami, Anh T Quach, and Aravind Prakash, *Binghamton University*
- DECAF++: Elastic Whole-System Dynamic Taint Analysis** 31
Ali Davanian, Zhenxiao Qi, Yu Qu, and Heng Yin, *University of California, Riverside*

Understanding Attacks

- Towards a First Step to Understand the Cryptocurrency Stealing Attack on Ethereum** 47
Zhen Cheng, *Zhejiang University*; Xinrui Hou, *Xidian University*; Runhuai Li and Yajin Zhou, *Zhejiang University*;
Xiapu Luo, *The Hong Kong Polytechnic University*; Jinku Li, *Xidian University*; Kui Ren, *Zhejiang University*
- Fingerprinting Tooling used for SSH Compromisation Attempts** 61
Vincent Ghiütte, Harm Griffioen, and Christian Doerr, *TU Delft*
- Timing Patterns and Correlations in Spontaneous SCADA Traffic for Anomaly Detection** 73
Chih-Yuan Lin and Simin Nadjm-Tehrani, *Linköping Universitet*

Defenses

- USBESAFE: An End-Point Solution to Protect Against USB-Based Attacks** 89
Amin Kharraz, *University of Illinois at Urbana Champaign*; Brandon L. Daley and Graham Z. Baker, *MIT Lincoln
Laboratory*; William Robertson and Engin Kirda, *Northeastern University*
- Minimal Kernel: An Operating System Architecture for TEE to Resist Board Level Physical Attacks** 105
Shijun Zhao, *Institute of Software Chinese Academy of Sciences*; Qianying Zhang, *Capital Normal University
Information Engineering College*; Yu Qin, Wei Feng, and Dengguo Feng, *Institute of Software Chinese Academy
of Sciences*
- ScaRR: Scalable Runtime Remote Attestation for Complex Systems** 121
Flavio Toffalini, *Singapore University of Technology and Design*; Eleonora Losiouk and Andrea Biondo, *University of
Padua*; Jianying Zhou, *Singapore University of Technology and Design*; Mauro Conti, *University of Padua*

Embedded Security

- Toward the Analysis of Embedded Firmware through Automated Re-hosting** 135
Eric Gustafson, *UC Santa Barbara*; Marius Muench, *EURECOM*; Chad Spensky, Nilo Redini, and Aravind Machiry,
UC Santa Barbara; Yanick Fratantonio, Davide Balzarotti, and Aurelien Francillon, *EURECOM*; Yung Ryn Choe,
Sandia National Laboratories; Christopher Kruegel and Giovanni Vigna, *UC Santa Barbara*
- CRYPTOREX: Large-scale Analysis of Cryptographic Misuse in IoT Devices** 151
Li Zhang, *Jinan University*; Jiongyi Chen, *The Chinese University of Hong Kong*; Wenrui Diao and Shanqing Guo,
Shandong University; Jian Weng, *Jinan University*; Kehuan Zhang, *The Chinese University of Hong Kong*
- PAtt: Physics-based Attestation of Control Systems** 165
Hamid Reza Ghaeini, *Singapore University of Technology and Design*; Matthew Chan, *Rutgers University*; Raad
Bahmani and Ferdinand Brasser, *TU Darmstadt*; Luis Garcia, *University of California, Los Angeles*; Jianying Zhou,
Singapore University of Technology and Design; Ahmad-Reza Sadeghi, *TU Darmstadt*; Nils Ole Tippenhauer, *CISPA,
Helmholtz Center for Information Security*; Saman Zonouz, *Rutgers University*

(continued on next page)

COMA: Communication and Obfuscation Management Architecture 181
Kimia Zamiri Azar, Farnoud Farahmand, Hadi Mardani Kamali, Shervin Roshanisefat, and Houman Homayoun,
George Mason University; William Diehl, *Virginia Tech*; Kris Gaj and Avesta Sasan, *George Mason University*

Privacy Enhancing Techniques

PRO-ORAM: Practical Read-Only Oblivious RAM 197
Shruti Tople, *Microsoft*; Yaoqi Jia, *Ziliqa Research*; Prateek Saxena, *NUS*

The DUSTER Attack: Tor Onion Service Attribution Based on Flow Watermarking with Track Hiding 213
Alfonso Iacovazzi, *ST Engineering-SUTD Cyber Security Laboratory, Singapore University of Technology and Design*;
Daniel Frassinelli, *CISPA, Helmholtz Center for Information Security, Germany*; Yuval Elovici, *Department of Software
and Information Systems Engineering and Cyber Security Research Center, Ben-Gurion University of the Negev, Israel,*
and *iTrust—Centre for Research in Cyber Security, Singapore University of Technology and Design, Singapore*

TALON: An Automated Framework for Cross-Device Tracking Detection 227
Konstantinos Solomos, *FORTH*; Panagiotis Ilia, *University of Illinois at Chicago*; Sotiris Ioannidis, *FORTH*;
Nicolas Kourtellis, *Telefonica Research*

Android Security I

Analysis of Location Data Leakage in the Internet Traffic of Android-based Mobile Devices 243
Nir Sivan, Ron Bitton, and Asaf Shabtai, *Ben Gurion University of the Negev*

Kindness is a Risky Business: On the Usage of the Accessibility APIs in Android 261
Wenrui Diao, *Shandong University*; Yue Zhang and Li Zhang, *Jinan University*; Zhou Li, *University of California, Irvine*;
Fenghao Xu, *The Chinese University of Hong Kong*; Xiaorui Pan, *Indiana University Bloomington*; Xiangyu Liu, *Alibaba
Inc.*; Jian Weng, *Jinan University*; Kehuan Zhang, *The Chinese University of Hong Kong*; XiaoFeng Wang, *Indiana
University Bloomington*

Automatic Generation of Non-intrusive Updates for Third-Party Libraries in Android Applications 277
Yue Duan, *Cornell University*; Lian Gao, Jie Hu, and Heng Yin, *University of California Riverside*

Machine Learning & Watermarking

Exploiting the Inherent Limitation of L_0 Adversarial Examples 293
Fei Zuo, Bokai Yang, Xiaopeng Li, Lannan Luo, and Qiang Zeng, *University of South Carolina*

NLP-EYE: Detecting Memory Corruptions via Semantic-Aware Memory Operation Function Identification 309
Jianqiang Wang, *Shanghai Jiao Tong University*; Siqi Ma, *CSIRO DATA61*; Yuanyuan Zhang and Juanru Li, *Shanghai
Jiao Tong University*; Zheyu Ma, *Northwestern Polytechnical University*; Long Mai, Tiancheng Chen, and Dawu Gu,
Shanghai Jiao Tong University

Robust Optimization-Based Watermarking Scheme for Sequential Data 323
Erman Ayday, *Case Western Reserve University and Bilkent University*; Emre Yilmaz, *Case Western Reserve University*;
Arif Yilmaz, *Bilkent University*

Malware

Smart Malware that Uses Leaked Control Data of Robotic Applications: The Case of Raven-II Surgical Robots 337
Keywhan Chung and Xiao Li, *University of Illinois at Urbana-Champaign*; Peicheng Tang, *Rose-Hulman Institute of
Technology*; Zeran Zhu, Zbigniew T. Kalbarczyk, Ravishankar K. Iyer, and Thenkurussi Kesavadas, *University of Illinois
at Urbana-Champaign*

SGXJail: Defeating Enclave Malware via Confinement 353
Samuel Weiser, Luca Mayr, Michael Schwarz, and Daniel Gruss, *Graz University of Technology*

Fluorescence: Detecting Kernel-Resident Malware in Clouds 367
Richard Li, *University of Utah*; Min Du, *University of California Berkeley*; David Johnson, Robert Ricci, Jacobus Van der
Merwe, and Eric Eide, *University of Utah*

DNS Security

Now You See It, Now You Don't: A Large-scale Analysis of Early Domain Deletions 383
Timothy Barron, Najmeh Miramirkhani, and Nick Nikiforakis, *Stony Brook University*

HinDom: A Robust Malicious Domain Detection System based on Heterogeneous Information Network with Transductive Classification..... 399

Xiaoqing Sun, Mingkai Tong, and Jiahai Yang, *Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing, China*; Liu Xinran, *National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing, China*; Liu Heng, *China Electronics Cyberspace Great Wall Co., Ltd, Beijing, China*

DomainScouter: Understanding the Risks of Deceptive IDNs..... 413

Daiki Chiba, Ayako Akiyama Hasegawa, and Takashi Koide, *NTT Secure Platform Laboratories*; Yuta Sawabe and Shigeki Goto, *Waseda University*; Mitsuaki Akiyama, *NTT Secure Platform Laboratories*

Attacks

Dynamically Finding Minimal Eviction Sets Can Be Quicker Than You Think for Side-Channel Attacks against the LLC..... 427

Wei Song, *Institute of Information Engineering, CAS*; Peng Liu, *Pennsylvania State University*

Time and Order: Towards Automatically Identifying Side-Channel Vulnerabilities in Enclave Binaries 443

Wubing Wang, Yinqian Zhang, and Zhiqiang Lin, *The Ohio State University*

Application level attacks on Connected Vehicle Protocols 459

Ahmed Abdo, Sakib Md Bin Malek, and Zhiyun Qian, *University of California, Riverside*; Qi Zhu, *Northwestern University*; Matthew Barth and Nael Abu-Ghazaleh, *University of California, Riverside*

Security in Data Centers and the Cloud

S3: A DFW-based Scalable Security State Analysis Framework for Large-Scale Data Center Networks 473

Abdulhakim Sabur, Ankur Chowdhary, and Dijiang Huang, *Arizona State University*; Myong Kang, Anya Kim, and Alexander Velazquez, *Naval Research Lab*

Container-IMA: A privacy-preserving Integrity Measurement Architecture for Containers..... 487

Wu Luo, Qingni Shen, Yutang Xia, and Zhonghai Wu, *Peking University, Beijing, China*

Fingerprinting SDN Applications via Encrypted Control Traffic..... 501

Jiahao Cao, *Tsinghua University and George Mason University*; Zijie Yang, *Tsinghua University*; Kun Sun, *George Mason University*; Qi Li, Mingwei Xu, *Tsinghua University*; Peiyi Han, *Beijing University of Posts and Telecommunications*

Android Security II

Exploring Syscall-Based Semantics Reconstruction of Android Applications.....517

Dario Nisi, *EURECOM*; Antonio Bianchi, *University of Iowa*; Yanick Fratantonio, *EURECOM*

Towards Large-Scale Hunting for Android Negative-Day Malware..... 533

Lun-Pin Yuan, *Penn State University*; Wenjun Hu, *Palo Alto Networks Inc.*; Ting Yu, *Qatar Computing Research Institute*; Peng Liu and Sencun Zhu, *Penn State University*

DroidScraper: A Tool for Android In-Memory Object Recovery and Reconstruction..... 547

Aisha Ali-Gombe, *Towson University*; Sneha Sudhakaran, *Louisiana State University*; Andrew Case, *Volatility Foundation*; Golden G. Richard III, *Louisiana State University*