

Network and Distributed System Security Symposium 2021 (NDSS'21)

Online
21-25 February 2021

Volume 1 of 2

ISBN: 978-1-7138-3761-9

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© (2021) by The Internet Society
All rights reserved.

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

For permission requests, please contact The Internet Society
at the address below.

The Internet Society
11710 Plaza America Drive, Suite 400
Reston, VA 20190
U.S.A.

Phone: (703) 439-2120
Fax: (703) 326-9881

www.internetsociety.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

TABLE OF CONTENTS

VOLUME 1

SESSION 1A: NETWORK SECURITY

Flexsealing BGP Against Route Leaks: Peerlock Active Measurement and Analysis.....	1
<i>Tyler McDaniel, Jared M. Smith, Max Schuchard</i>	
A Devil of a Time: How Vulnerable is NTP to Malicious Timeservers?	17
<i>Yarin Perry, Neta Rozen-Schiff, Michael Schapira</i>	
OblivSketch: Oblivious Network Measurement as a Cloud Service	35
<i>Shangqi Lai, Xingliang Yuan, Joseph Liu, Xun Yi, Qi Li, Dongxi Liu, Nepal Surya</i>	
ROV++: Improved Deployable Defense against BGP Hijacking.....	53
<i>Reynaldo Morillo, Justin Furuness, Cameron Morris, James Breslin, Amir Herzberg, Bing Wang</i>	
Trust the Crowd: Wireless Witnessing to Detect Attacks on ADS-B-Based Air-Traffic Surveillance	71
<i>Kai Jansen, Liang Niu, Nian Xue, Ivan Martinovic, Christina Pöpper</i>	

SESSION 1B: PROGRAM ANALYSIS 1

Towards Measuring Supply Chain Attacks on Package Managers for Interpreted Languages	88
<i>Ruian Duan, Omar Alrawi, Ranjita Pai Kasturi, Ryan Elder, Brendan Saltaformaggio, Wenke Lee</i>	
Processing Dangerous Paths – On Security and Privacy of the Portable Document Format.....	105
<i>Jens Müller, Dominik Noss, Christian Mainka, Vladislav Mladenov, Jörg Schwenk</i>	
XDA: Accurate, Robust Disassembly with Transfer Learning	121
<i>Kexin Pei, Jonas Guan, David Williams-King, Junfeng Yang, Suman Jana</i>	
Shadow Attacks: Hiding and Replacing Content in Signed PDFs.....	139
<i>Christian Mainka, Vladislav Mladenov, Simon Rohlmann</i>	
KUBO: Precise and Scalable Detection of User-triggerable Undefined Behavior Bugs in OS Kernel.....	156
<i>Changming Liu, Yaohui Chen, Long Lu</i>	

SESSION 1C: PRIVACY

Awakening the Web's Sleeper Agents: Misusing Service Workers for Privacy Leakage	171
<i>Soroush Karami, Panagiotis Ilia, Jason Polakis</i>	
All the Numbers are US: Large-scale Abuse of Contact Discovery in Mobile Messengers.....	187
<i>Christoph Hagen, Christian Weinert, Christoph Sendner, Alexandra Dmitrienko, Thomas Schneider</i>	
Improving Signal's Sealed Sender	204
<i>Ian Martiny, Gabriel Kaptchuk, Adam Aviv, Dan Roche, Eric Wustrow</i>	

Tales of Favicons and Caches: Persistent Tracking in Modern Browsers	222
<i>Konstantinos Solomos, John Kristoff, Chris Kanich, Jason Polakis</i>	

SESSION 2A: NETWORK POLICIES

Reining in the Web's Inconsistencies with Site Policy	241
<i>Stefano Calzavara, Tobias Urban, Dennis Tatang, Marius Steffens, Ben Stock</i>	
From WHOIS to WHOWAS: A Large-Scale Measurement Study of Domain Registration Privacy under the GDPR	257
<i>Chaoyi Lu, Baojun Liu, Yiming Zhang, Zhou Li, Fenglu Zhang, Haixin Duan, Yingliu, Joann Qiongna Chen, Jinjin Liang, Zaifeng Zhang, Shuang Hao, Min Yang</i>	
Understanding the Growth and Security Considerations of ECS	275
<i>Athanasios Kountouras, Panagiotis Kintis, Athanasios Avgetidis, Thomas Papastergiou, Charles Lever, Michalis Polychronakis, Manos Antonakakis</i>	
Mondrian: Comprehensive Inter-domain Network Zoning Architecture	291
<i>Jonghoon Kwon, Claude Hahni, Patrick Bamert, Adrian Perrig</i>	

SESSION 2B: PROGRAM ANALYSIS 2

Bringing Balance to the Force: Dynamic Analysis of the Android Application Framework	307
<i>Abdallah Dawoud, Sven Bugiel</i>	
SymQEMU: Compilation-based Symbolic Execution for Binaries	325
<i>Sebastian Poeplau, Aurélien Francillon</i>	
TASE: Reducing Latency of Symbolic Execution with Transactional Memory	343
<i>Adam Humphries, Kartik Cating-Subramanian, Michael K. Reiter</i>	
Refining Indirect Call Targets at the Binary Level.....	358
<i>Sun Hyoung Kim, Cong Sun, Dongrui Zeng, Gang Tan</i>	

SESSION 2C: CRYPTO

Obfuscated Access and Search Patterns in Searchable Encryption	376
<i>Zhiwei Shang, Simon Oya, Andreas Peter, Florian Kerschbaum</i>	
More than a Fair Share: Network Data Remanence Attacks against Secret Sharing based Schemes.....	394
<i>Leila Rashidi, Daniel Kostecki, Alexander James, Anthony Peterson, Majid Ghaderi, Samuel Jero, Cristina Nita-Rotaru, Hamed Okhravi, Reihaneh Safavi-Naini</i>	
Forward and Backward Private Conjunctive Searchable Symmetric Encryption	408
<i>Sikhar Patranabis, Debdeep Mukhopadhyay</i>	
Practical Non-Interactive Searchable Encryption with Forward and Backward Privacy	426
<i>Shi-Feng Sun, Ron Steinfeld, Shangqi Lai, Xingliang Yuan, Amin Sakzad, Joseph Liu, Surya Nepal, Dawu Gu</i>	

SESSION 3A: WEB SECURITY

Zoom on the Keystrokes: Exploiting Video Calls for Keystroke Inference Attacks	444
<i>Mohd Sabra, Anindya Maiti, Murtuza Jadliwala</i>	
Deceptive Deletions for Protecting Withdrawn Posts on Social Media Platforms	462
<i>Mohsen Minaei, S Chandra Mouli, Mainack Mondal, Bruno Ribeiro, Aniket Kate</i>	
Who's Hosting the Block Party? Studying Third-Party Blockage of CSP and SRI.....	480
<i>Marius Steffens, Marius Musch, Martin Johns, Ben Stock</i>	
To Err.Is Human: Characterizing the Threat of Unintended URLs in Social Media.....	497
<i>Beliz Kaleli, Brian Kondracki, Manuel Egele, Nick Nikiforakis, Gianluca Stringhini</i>	
SerialDetector: Principled and Practical Exploration of Object Injection Vulnerabilities for the Web.....	512
<i>Mikhail Shcherbakov, Musard Balliu</i>	

SESSION 3B: MOBILE SECURITY

The Abuser Inside Apps: Finding the Culprit Committing Mobile Ad Fraud.....	530
<i>Joongyum Kim, Jung-Hwan Park, Soeul Son</i>	
Your Phone is My Proxy: Detecting and Understanding Mobile Proxy Networks	546
<i>Xianghang Mi, Siyuan Tang, Zhengyi Li, Xiaojing Liao, Feng Qian, Xiaofeng Wang</i>	
Understanding Worldwide Private Information Collection on Android.....	564
<i>Yun Shen, Pierre-Antoine Vervier, Gianluca Stringhini</i>	
On the Insecurity of SMS One-Time Password Messages against Local Attackers in Modern Mobile Devices.....	580
<i>Zeyu Lei, Yuhong Nan, Yanick Fratantonio, Antonio Bianchi</i>	
Preventing and Detecting State Inference Attacks on Android	598
<i>Andrea Possemato, Dario Nisi, Yanick Fratantonio</i>	

SESSION 3C: BLOCKCHAINS

As Strong as Its Weakest Link: How to Break Blockchain DApps at RPC Service.....	616
<i>Kai Li, Jiaqi Chen, Xianghong Liu, Yuzhe Tang, Xiaofeng Wang, Xiapu Luo</i>	
RandRunner: Distributed Randomness from Trapdoor VDFs with Strong Uniqueness	634
<i>Philipp Schindler, Aljosha Judmayer, Markus Hittmeir, Nicholas Stifter, Edgarweippl</i>	
LaKSA: A Probabilistic Proof-of-Stake Protocol.....	652
<i>Daniel Reijbergen, Pawel Szalachowski, Junming Ke, Zengpeng Li, Jianying Zhou</i>	
SquirRL: Automating Attack Analysis on Blockchain Incentive Mechanisms with Deep Reinforcement Learning.....	670
<i>Charlie Hou, Mingxun Zhou, Yan Ji, Phil Daian, Florian Tramèr, Giulia Fanti, Ari Juels</i>	
Bitcontracts: Supporting Smart Contracts in Legacy Blockchains.....	688
<i>Karl Wüst, Loris Diana, Kari Kostianen, Ghassan Karame, Sinisa Matetic, Srdjan Capkun</i>	

SESSION 4A: NETWORK PROTOCOLS

- QPEP: An Actionable Approach to Secure and Performant Broadband From Geostationary Orbit 706
James Pavur, Martin Strohmeier, Vincent Lenders, Ivan Martinovic
- A Formal Analysis of the FIDO UAF Protocol..... 723
Haonan Feng, Hui Li, Xuesong Pan, Ziming Zhao
- PHOENIX: Device-Centric Cellular Network Protocol Monitoring using Runtime Verification 738
Mitziu Echeverria, Zeeshan Ahmed, Bincheng Wang, M. Fareed Arif, Syed Rafiulhussain, Omar Chowdhury

VOLUME 2

- The Bluetooth CYBORG: Analysis of the Full Human-Machine Passkey Entry AKE Protocol..... 756
Michael Troncoso, Britta Hale
- NetPlier: Probabilistic Network Protocol Reverse Engineering from Message Traces..... 774
Yapeng Ye, Zhuo Zhang, Fei Wang, Xiangyu Zhang, Dongyan Xu

SESSION 4B: SIDE-CHANNELS AND SPECULATION

- Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an Electromagnetic Side Channel..... 792
Zhuoran Liu, Niels Samwel, Léo Weissbart, Zhengyu Zhao, Dirk Lauret, Lejlabatina, Martha Larson
- Rosita: Towards Automatic Elimination of Power-Analysis Leakage in Ciphers..... 807
Madura A. Shelton, Niels Samwel, Lejla Batina, Francesco Regazzoni, Markus Wagner, Yuval Yarom
- Hunting the Haunter — Efficient Relational Symbolic Execution for Spectre with Haunted RelSE..... 824
Lesly-Ann Daniel, Sébastien Bardin, Tamara Rezk
- SpecTaint: Speculative Taint Analysis for Discovering Spectre Gadgets 841
Zhenxiao Qi, Qian Feng, Yueqiang Cheng, Mengjia Yan, Peng Li, Heng Yin, Tao Wei

SESSION 4C: MALWARE AND CYBER-CRIME

- Understanding and Detecting International Revenue Share Fraud..... 855
Merve Sahin, Aurélien Francillon
- Differential Training: A Generic Framework to Reduce Label Noises for Android Malware Detection 871
Jiayun Xu, Yingjiu Li, Robert H. Deng
- MINOS: A Lightweight Real-Time Cryptojacking Detection System..... 885
Faraz Naseem, Ahmet Aris, Leonardo Babun, Ege Tekiner, A. Selcuk Uluagac
- Does Every Second Count? Time-based Evolution of Malware Behavior in Sandboxes 900
Alexander Küchler, Alessandro Mantovani, Yufei Han, Leyla Bilge, Davide Balzarotti

SESSION 5A: “SMART” HOME

- Hey Alexa, is this Skill Safe?: Taking a Closer Look at the Alexa Skill Ecosystem 918
Christopher Lentzsch, Sheel Jayesh Shah, Benjamin Andow, Martin Degeling, Anupam Das, William Enck
- IoTSafe: Enforcing Safety and Security Policy with Real IoT Physical Interaction Discovery 936
Wenbo Ding, Hongxin Hu, Long Cheng
- PFirewall: Semantics-Aware Customizable Data Flow Control for Smart Home Privacy Protection 954
Haotian Chi, Qiang Zeng, Xiaojiang Du, Lannan Luo
- EarArray: Defending against DolphinAttack via Acoustic Attenuation..... 972
Guoming Zhang, Xiaoyu Ji, Xinfeng Li, Gang Qu, Wenyuan Xu

SESSION 5B: SOFTWARE DEFENSES

- POP and PUSH: Demystifying and Defending against (Mach) Port-oriented Programming..... 986
Min Zheng, Xiaolong Bai, Yajin Zhou, Chao Zhang, Fuping Qu
- Доверьяй, но проверьяй: SFI safety for native-compiled Wasm 1003
Evan Johnson, David Thien, Yousef Alhessi, Shravan Narayan, Fraser Brown, Sorin Lerner, Tyler McMullen, Stefan Savage, Deian Stefan
- Detecting Kernel Memory Leaks in Specialized Modules with Ownership Reasoning 1019
Navid Emamdoost, Qiushi Wu, Kangjie Lu, Stephen McCamant

SESSION 5C: MACHINE LEARNING

- Let's Stride Blindfolded in a Forest: Sublinear Multi-Client Decision Trees Evaluation 1037
Jack P. K. Ma, Raymond K. H. Tai, Yongjun Zhao, Sherman S. M. Chow
- Practical Blind Membership Inference Attack via Differential Comparisons 1055
Bo Hui, Yuchen Yang, Haolin Yuan, Philippe Burlina, Neil Zhenqiang Gong, Yinzhicao
- GALA: Greedy ComputAtion for Linear Algebra in Privacy-Preserved Neural Networks 1072
Qiao Zhang, Chunsheng Xin, Hongyi Wu
- FARE: Enabling Fine-grained Attack Categorization under Low-quality Labeled Data 1088
Junjie Liang, Wenbo Guo, Tongbo Luo, Vasant Honavar, Gang Wang, Xinyu Xing

SESSION 6A: FUZZING

- PGFUZZ: Policy-Guided Fuzzing for Robotic Vehicles..... 1106
Hyungsub Kim, Muslum Ozgur Ozmen, Antonio Bianchi, Z. Berkay Celik, Dongyan Xu
- Favocado: Fuzzing Binding Code of JavaScript Engines Using Semantically Correct TestCases..... 1124
Sung Ta Dinh, Haehyun Cho, Kyle Martin, Adam Oest, Yihui Zeng, Alexandros Kapravelos, Tiffany Bao, Ruoyu Wang
- WINNIE: Fuzzing Windows Applications with Harness Synthesis and Fast Cloning 1139
Jinho Jung, Stephen Tong, Hong Hu, Jungwon Lim, Yonghwi Jin, Taesoo Kim

Reinforcement Learning-based Hierarchical Seed Scheduling for Greybox Fuzzing 1156
Jinghan Wang, Chengyu Song, Heng Yin

SESSION 6B: EMBEDDED SECURITY

Evading Voltage-Based Intrusion Detection on Automotive CAN 1173
Rohit Bhatia, Vireshwar Kumar, Khaled Serag, Z. Berkay Celik, Mathias Payer, Dongyan Xu

HERA: Hotpatching of Embedded Real-time Applications 1190
Christian Niesler, Sebastian Surminski, Lucas Davi

From Library Portability to Para-rehosting: Natively Executing Microcontroller Software on
Commodity Hardware 1206
Wenqiang Li, Le Guan, Jingqiang Lin, Jiameng Shi, Fengjun Li

BaseSpec: Comparative Analysis of Baseband Software and Cellular Specifications for L3
Protocols 1224
Eunsoo Kim, Dongkwan Kim, Cheoljun Park, Insu Yun, Yongdae Kim

SESSION 6C: FEDERATED LEARNING AND POISONING ATTACKS

POSEIDON: Privacy-Preserving Federated Neural Network Learning 1242
Sinem Sav, Apostolos Pyrgelis, Juan Ramón Troncoso-Pastoriza, David Froelicher, Jean-Philippe Bossuat, Joao Sa Sousa, Jean-Pierre Hubaux

FLTrust: Byzantine-robust Federated Learning via Trust Bootstrapping 1260
Xiaoyu Cao, Minghong Fang, Jia Liu, Neil Zhenqiang Gong

Manipulating the Byzantine: Optimizing Model Poisoning Attacks and Defenses for Federated
Learning 1278
Virat Shejwalkar, Amir Houmansadr

Data Poisoning Attacks to Deep Learning Based Recommender Systems 1296
Hai Huang, Jiaming Mu, Neil Zhenqiang Gong, Qi Li, Bin Liu, Mingwei Xu

SESSION 7A: FORENSICS AND AUDITS

C²SR Cybercrime Scene Reconstruction for Post-mortem Forensic Analysis 1313
Yonghwi Kwon, Weihang Wang, Jinho Jung, Kyu Hyung Lee, Roberto Perdisci

ALchemist: Fusing Application and Audit Logs for Precise Attack Provenance without
Instrumentation 1331
Le Yu, Shiqing Ma, Zhuo Zhang, Guanhong Tao, Xiangyu Zhang, Dongyan Xu, Vincent E. Urias, Han Wei Lin, Gabriela Ciocarlie, Vinod Yegneswaran, Ashish Gehani

WATSON: Abstracting Behaviors from Audit Logs via Aggregation of Contextual Semantics 1349
Jun Zeng, Zheng Leong Chua, Yinfang Chen, Kaihang Ji, Zhenkai Liang, Jian Mao

SESSION 7B: TRUSTED COMPUTING

DOVE: A Data-Oblivious Virtual Environment 1367
Hyun Bin Lee, Tushar Jois, Christopher Fletcher, Carl A. Gunter

CHANCEL: Efficient Multi-client Isolation Under Adversarial Programs.....	1384
<i>Adil Ahmad, Juhee Kim, Jaebaek Seo, Insik Shin, Pedro Fonseca, Byoungyoung Lee</i>	
Emilia: Catching Iago in Legacy Code.....	1402
<i>Rongzhen Cui, Lianying Zhao, David Lie</i>	

SESSION 7C: MACHINE LEARNING APPLICATIONS

CV-Inspector: Towards Automating Detection of Adblock Circumvention	1419
<i>Hieu Le, Athina Markopoulou, Zubair Shafiq</i>	
FlowLens: Enabling Efficient Flow Classification for ML-based Network Security Applications	1437
<i>Diogo Barradas, Nuno Santos, Luis Rodrigues, Salvatore Signorello, Fernando M. V. Ramos, André Madeira</i>	
PrivacyFlash Pro: Automating Privacy Policy Generation for Mobile Apps	1455
<i>Sebastian Zimmeck, Rafael Goldstein, David Baraka</i>	
Towards Understanding and Detecting Cyberbullying in Real-world Images	1473
<i>Nishant Vishwamitra, Hongxin Hu, Feng Luo, Long Cheng</i>	

ADDITIONAL PAPERS

PhantomCache: Obfuscating Cache Conflicts with Localized Randomization.....	1491
<i>Qinhan Tan, Zhihua Zeng, Kai Bu, Kui Ren</i>	
UISCOPE: Accurate, Instrumentation-free, and Visible Attack Investigation for GUI Applications.....	1508
<i>Runqing Yang, Shiqing Ma, Haitao Xu, Xiangyu Zhang, Yan Chen</i>	
SODA: A Generic Online Detection Framework for Smart Contracts.....	1526
<i>Ting Chen, Rong Cao, Ting Li, Xiapu Luo, Guofei Gu, Yufei Zhang, Zhou Liao, Hang Zhu, Gang Chen, Zheyuan He, Yuxing Tang, Xiaodong Lin, Xiaosong Zhang</i>	

Author Index