Network and Distributed System Security Symposium 2017

San Diego, California, USA
26 February - 1 March 2017

Volume 1 of 2

ISBN: 978-1-7138-2194-6

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© (2017) by The Internet Society
All rights reserved.

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

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

Proceedings of the 2017 Network and Distributed System Security Symposium

Table of Contents

General Chair's Message
Program Chair's Message
Organizing Committee
Program Committee
Steering Group

Keynote Speaker: *J. Alex Halderman, Professor, University of Michigan*

Session 1: Applied Crypto and Cryptocurrencies

IO-DSSE: Scaling Dynamic Searchable Encryption to Millions of Indexes By Improving Locality...1
I. Miers, P.Mohassel

ObliviSync: Practical Oblivious File Backup and Synchronization...14
A.J. Aviv, S. Geol Choi, T. Mayberry, D.S. Roche

TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub...29
E. Heilman, L.Alshenibr, F. Baldimtsi, A. Scafuro, S. Goldberg

P2P Mixing and Unlinkable Bitcoin Transactions...44
T. Ruffing, P. Moreno-Sanchez, A. Kate

SilentWhispers: Enforcing Security and Privacy in Decentralized Credit Networks...59
G. Malavolta, P. Moreno-Sanchez, A. Kate, M. Maffei

Session 2A: Virtualization and SDN

DELTA: A Security Assessment Framework for Software-Defined Networks...74
S. Lee, C. Yoon, C. Lee, S. Shin, V. Yegneswaran, P. Porras

PSI: Precise Security Instrumentation for Enterprise Networks...89
T. Yu, S. K. Fayaz, M. Collins, V. Sekar, S. Seshan

On the Safety and Efficiency of Virtual Firewall Elasticity Control...104
J. Deng, H. Li, H.Hu, K.-C. Wang, G.-J. Ahn, Z. Zhao, W. Han

Deconstructing Xen...119
L. Shi, Y. Wu, Y. Xia, N. Dautenhahn, H. Chen, B. Zang, H. Guan, J. Li

Session 2B: Web Security

Thou Shalt Not Depend on Me: Analysing the Use of Outdated JavaScript Libraries on the Web...134
T. Lauinger, A. Chaabane, S. Arshad, W. Robertson, C. Wilson, E. Kirda

Enabling Reconstruction of Attacks on Users via Efficient Browsing Snapshots...149
P. Vadrevu, J. Liu, B. Li, B. Rahbarinia, K. H. Lee, R. Perdisci

(Cross-)Browser Fingerprinting via OS and Hardware Level Features...164
Y. Cao, S. Li, E. Wijmans

Fake Co-visitation Injection Attacks to Recommender Systems...179
G. Yang, N. Z. Gong, Y. Cai

Session 3A: User Authentication

Broken Hearted: How To Attack ECG Biometrics...194
S. Eberz, N. Paoletti, M. Roeschlin, A. Patané, M. Kwiatkowska, I. Martinovic

Towards Implicit Visual Memory-Based Authentication...209
C. Castelluccia, M. Dürmuth, M. Golla, F. Deniz

KEH-Gait: Towards a Mobile Healthcare User Authentication System by Kinetic Energy Harvesting...224
W. Xu, G. Lan, Q. Lin, S. Khalifa, N. Bergmann, M. Hassan, W. Hu

A Large-scale Analysis of the Mnemonic Password Advice...239
J. Kiesel, B. Stein, S. Lucks

Cracking Android Pattern Lock in Five Attempts...252
G. Ye, Z. Tang, D. Fang, X. Chen, K. I. Kim, B. Taylor, Z. Wang

Session 3B: Malware

Dial One for Scam: A Large-Scale Analysis of Technical Support Scams...267
N. Miramirkhani, O. Starov, N. Nikiforakis

Automated Synthesis of Semantic Malware Signatures using Maximum Satisfiability...282
Y. Feng, O. Bastani

MAMADROID: Detecting Android Malware by Building Markov Chains of Behavioral Models...297
E. Mariconti, L. Onwuzurike, P. Andriotis, E. De Cristofaro, G. Ross, G. Stringhini

A Broad View of the Ecosystem of Socially Engineered Exploit Documents...312
S. Le Blond, C. Gilbert, U. Upadhyay, M. Gomez Rodriguez, D. Choffnes

Catching Worms, Trojan Horses and PUPs: Unsupervised Detection of Silent Delivery Campaigns...327
B. J. Kwon, V. Srinivas, A. Deshpande, T. Dumitras

Session 4A: TLS et al.

Measuring small subgroup attacks against Diffie-Hellman...342
L. Valenta, D. Adrian, A. Sanso, S. Cohney, J. Fried, M. Hastings, J. A. Halderman, N. Heninger

Indiscreet Logs: Persistent Diffie-Hellman Backdoors in TLS...357
K. Dorey, N. Chang-Fong, A. Essex

WireGuard: Next Generation Kernal Network Tunnel...371
J. A. Donenfeld

The Security Impact of HTTPS Interception...383
Z. Durumeric, Z. Ma, D. Springall, R. Barnes, N. Sullivan, E. Bursztein, M. Bailey J. A. Halderman, V. Paxson

Session 4B: Secure Computation

Fast Actively Secure OT Extension for Short Secrets...397
A. Patra, P. Sarkar, A. Suresh

Constant Round Maliciously Secure 2PC with Function-independent Preprocessing using LEGO...412
J. B. Nielsen, T. Schneider, R. Trifiletti

Pushing the Communication Barrier in Secure Computation using Lookup Tables...427
G. Dessouky, F. Koushanfar, A.-R. Sadeghi, T. Schneider, S. Zeitouni, M. Zohner

Using Fully Homomorphic Encryption for Statistical Analysis of Categorical, Ordinal and Numerical Data...442
W. Lu, S. Kawasaki, J. Sakuma

Session 5A: Mobile Privacy and Security

Dark Hazard; Learning-based, Large-scale Discovery of Hidden Sensitive Operations in Android Apps...457
X. Pan, X. Wang, Y. Duan, X.F. Wang, H. Yin

Show Me the Money! Finding Flawed Implementations of Third-party In-app Payment in Android Apps...472
W. Yang, Y. Zhang, J. Li, H. Liu, Q. Wang, Y. Zhang, D. Gu

WindowGuard: Systematic Protection of GUI Security in Android...487
C. Ren, P. Liu, S. Zhu

Obfuscation-Resilient Privacy Leak Detection for Mobile Apps Through Differential Analysis...500
A. Continella, Y. Fratantonio, M. Lindorfer, A. Puccetti, A. Zand, C. Kruegel, G. Vigna

Automated Analysis of Privacy Requirements for Mobile Apps...515
S. Zimmeck, Z. Wang, L. Zou, R. Iyengar, B. Liu, F. Shaub, S. Wilson, N. Sadeh S. M. Bellovin, J. Reidenberg

Session 5B: Software and System Security (Part 1)

Dachshund: Digging for and Securing Against (Non-)Blinded Constants in JIT Code...530
G. Maisuradze, M. Backes, C. Rossow

SafeInit: Comprehensive and Practical Mitigation of Uninitialized Read Vulnerabilities...545
A. Milburn, H. Bos, C. Giuffrida

MARX: Uncovering Class Hierarchies in C++ Programs...560
A. Pawlowski, M.Contag, V. van der Veen, C. Ouwehand, T. Holz, H. Bos, E. Athanasopoulos, C. Giuffrida

PT-Rand: Practical Mitigation of Data-only Attacks against Page Tables...575
L. Davi, D. Gens, C. Liebchen, A.-R. Sadeghi

Dynamic Virtual Address Range Adjustment for Intra-Level Privilege Separation on ARM...590
Y. Cho, D. Kwon, H. Yi, Y. Paek

Session 6A: Cloud and Potpourri

Hello from the Other Side: SSH over Robust Cache Covert Channels in the Cloud...605
C. Maurice, M. Weber, M. Schwarz, L. Giner, D. Gruss, C. A. Boano, S. Mangard, K. Römer

Dynamic Differential Location Privacy with Personalized Error Bounds...620
L. Yu, L. Liu, C. Pu

Are We There Yet? On RPKI's Deployment and Security...635
Y. Gilad, A. Cohen, A. Herzberg, M. Schapira, H.Shulman

TenantGuard: Scalable Runtime Verification of Cloud-Wide VM-Level Network Isolation...650
Y. Wang, T. Madi, S. Majumdar, Y. Jarraya, A. Alimohammadifar, M. Pourzandi L. Wang, M. Debbabi

Session 6B: Tor

Dissecting Tor Bridges: A Security Evaluation of their Private and Public Infrastructures...665
S. Matic, C. Troncoso, J. Caballero

The Effect of DNS on Tor's Anonymity...680
B. Greschbach, T. Pulls, L.M. Roberts, P. Winter, N. Feamster

Avoding The Man on the Wire: Improving Tor's Security with Trust-Aware Path Selection...695
A. Johnson, R. Jansen, A. D. Jaggard, J. Feigenbaum, P. Syverson

HisTorε: Differentially Private and Robust Statistics Collection for Tor...710
A. Mani, M. Sherr

Session 7: Trusted Execution Environments

SGX-Shield: Enabling Address Space Layout Randomization for SGX Programs...725
J. Seo, B. Lee, S. Kim. M.-W. Shih, I. Shin, D. Han, T. Kim

T-SGX: Eradicating Controlled-Channel Attacks Against Enclave Programs...740
M.-W. Shih, S. Lee, T. Kim, M. Peinado

BOOMERANG: Exploiting the Semantic Gap in Trusted Execution Environments...755
A. Machiry, E. Gustafson, C. Spensky, C. Salls, N. Stephens, R. Wang,
A. Bianchi, Y. R. Choe, C. Kruegel, G. Vigna

HOP: Hardware makes Obfuscation Practical...770
K. Nayak, C.W. Fletcher, L. Ren, N. Chandran, S. Lokam, E. Shi, V. Goyal

PANOPLY: Low-TCB Linux Applications With SGX Enclaves...785
S. Shinde, D. L. Tien, S. Tople, P. Saxena

Keynote Speaker: *Trent Adams, Director of Information Security, PayPal*

Session 8: Cyberphysical Security

Hey, My Malware Knows Physics! Attacking PLCs with Physical Model Aware Rootkit...800
L. Garcia, F. Brasser, M. H. Cintuglu, A.-R. Sadeghi, O. Mohammed,
S.A. Zonouz

ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms...815
Y.J. Jia, Q.A. Chen, S.i Wang, A. Rahmati, E. Fernandes, Z.M. Mao,
A. Prakash

FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild...830
Z. Li, W. Wang, C. Wilson, J. Chen, C. Qian, T. Jung, L. Zhang, K. Liu, X. Li, Y. Liu

Internet-scale Probing of CPS: Inference, Characterization and Orchestration Analysis...845
C. Fachkha, E. Bou-Harb, A. Keliris, N. Memon, M. Ahamad

Wi-Fly? : Detecting Privacy Invasion Attacks by Consumer Drones...860
S. Birnbach, R. Baker, I. Martinovic

Session 9: Attacks

ASLR on the Line: Practical Cache Attacks on the MMU...875
B. Gras, K. Razavi, E. Bosman, H. Box, C. Giuffrida

Unleashing Use-Before-Initialization Vulnerabilities in the Linux Kernel Using Targeted Stack Spraying...890
K. Lu, M.-T. Walter, D. Pfaff, S. Nürnberger, W. Lee, M. Backes

Address-Oblivious Code Reuse: On the Effectiveness of Leakage-Resilient Diversity...905
R. Rudd, R. Skowyra, D. Bigelow, V. Dedhia, T. Hobson, S. Crane, C. Liebchen, P. Larsen, L. Davi, M. Franz, A.-R. Sadeghi, H. Okhravi

An Evil Copy: How the Loader Betrays You...920
X. Ge, M. Payer, T. Jaeger

Session 10: Software and System Security (Part II)

Stack Bounds Protection with Low Fat Pointers...934
G.J. Duck, R. H. C. Yap, L. Cavallaro

VUzzer: Application-aware Evolutionary Fuzzing...949
S. Rawat, V. Jain, A. Kumar, L. Cojocar, C. Giuffrida, H. Bos

Self Destructing Exploit Executions via Input Perturbation...963
Y. Kwon, B. Saltaformaggio, I L. Kim, K. H. Lee, X. Zhang, D. Xu

A Call to ARMs: Understanding the Costs and Benefits of JIT Spraying Mitigations...978
W. Lian, H. Shacham, S. Savage

Ramblr: Making Reassembly Great Again...993
R. Wang, Y. Shoshitaishvili, A. Bianchi, A. Machiry, J. Grosen, P. Grosen, C. Kruegel, G. Vigna