

2016 IEEE Symposium on Security and Privacy (SP 2016)

**San Jose, California, USA
22-26 May 2016**

Pages 1-505



**IEEE Catalog Number: CFP16020-POD
ISBN: 978-1-5090-0825-4**

**Copyright © 2016 by the Institute of Electrical and Electronics Engineers, Inc
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

******This publication is a representation of what appears in the IEEE Digital Libraries. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP16020-POD
ISBN (Print-On-Demand):	978-1-5090-0825-4
ISBN (Online):	978-1-5090-0824-7
ISSN:	1081-6011

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
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

2016 IEEE Symposium on Security and Privacy

SP 2016

Table of Contents

Message from the General Chair.....	xi
Message from the Program Committee Co-Chairs.....	xiv
Organizing Committee.....	xv
Program Committee.....	xvii
External Reviewers.....	xix

Hardware and Private Execution

HDFI: Hardware-Assisted Data-Flow Isolation	1
<i>Chengyu Song, Hyungon Moon, Monjur Alam, Insu Yun, Byoungyoung Lee, Taesoo Kim, Wenke Lee, and Yunheung Paek</i>	
A2: Analog Malicious Hardware	18
<i>Kaiyuan Yang, Matthew Hicks, Qing Dong, Todd Austin, and Dennis Sylvester</i>	
Cache Storage Channels: Alias-Driven Attacks and Verified Countermeasures	38
<i>Roberto Guanciale, Hamed Nemati, Christoph Baumann, and Mads Dam</i>	
Shreds: Fine-Grained Execution Units with Private Memory	56
<i>Yaohui Chen, Sebassujeen Reymondjohnson, Zhichuang Sun, and Long Lu</i>	
CaSE: Cache-Assisted Secure Execution on ARM Processors	72
<i>Ning Zhang, Kun Sun, Wenjing Lou, and Y. Thomas Hou</i>	

Analyze Me

Back in Black: Towards Formal, Black Box Analysis of Sanitizers and Filters	91
<i>George Argyros, Ioannis Stais, Aggelos Kiayias, and Angelos D. Keromytis</i>	
LAVA: Large-Scale Automated Vulnerability Addition	110
<i>Brendan Dolan-Gavitt, Patrick Hulin, Engin Kirda, Tim Leek, Andrea Mambretti, Wil Robertson, Frederick Ulrich, and Ryan Whelan</i>	
Prepose: Privacy, Security, and Reliability for Gesture-Based Programming	122
<i>Lucas Silva Figueiredo, Benjamin Livshits, David Molnar, and Margus Veanes</i>	

SOK: (State of) The Art of War: Offensive Techniques in Binary Analysis	138
<i>Yan Shoshitaishvili, Ruoyu Wang, Christopher Salls, Nick Stephens, Mario Polino, Andrew Dutcher, John Grosen, Siji Feng, Christophe Hauser, Christopher Kruegel, and Giovanni Vigna</i>	
Helping Johnny to Analyze Malware: A Usability-Optimized Decompiler and Malware Analysis User Study	158
<i>Khaled Yakdan, Sergej Dechand, Elmar Gerhards-Padilla, and Matthew Smith</i>	
Oblivious and Snarky	
A Practical Oblivious Map Data Structure with Secure Deletion and History Independence	178
<i>Daniel S. Roche, Adam Aviv, and Seung Geol Choi</i>	
TaoStore: Overcoming Asynchronicity in Oblivious Data Storage	198
<i>Cetin Sahin, Victor Zakhary, Amr El Abbadi, Huijia Lin, and Stefano Tessaro</i>	
Revisiting Square-Root ORAM: Efficient Random Access in Multi-party Computation	218
<i>Samee Zahur, Xiao Wang, Mariana Raykova, Adrià Gascón, Jack Doerner, David Evans, and Jonathan Katz</i>	
Cinderella: Turning Shabby X.509 Certificates into Elegant Anonymous Credentials with the Magic of Verifiable Computation	235
<i>Antoine Delignat-Lavaud, Cédric Fournet, Markulf Kohlweiss, and Bryan Parno</i>	
PhotoProof: Cryptographic Image Authentication for Any Set of Permissible Transformations	255
<i>Assa Naveh and Eran Tromer</i>	
Call Me on Usable Security	
I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security	272
<i>Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek</i>	
You Get Where You're Looking for: The Impact of Information Sources on Code Security	289
<i>Yasemin Acar, Michael Backes, Sascha Fahl, Doowon Kim, Michelle L. Mazurek, and Christian Stransky</i>	
Users Really Do Plug in USB Drives They Find	306
<i>Matthew Tischer, Zakir Durumeric, Sam Foster, Sunny Duan, Alec Mori, Elie Bursztein, and Michael Bailey</i>	
SoK: Everyone Hates Robocalls: A Survey of Techniques Against Telephone Spam	320
<i>Huahong Tu, Adam Doupe, Ziming Zhao, and Gail-Joon Ahn</i>	

Sending Out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways	339
<i>Bradley Reaves, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin R. B. Butler</i>	

Phoning it in

Following Devil’s Footprints: Cross-Platform Analysis of Potentially Harmful Libraries on Android and iOS	357
<i>Kai Chen, Xueqiang Wang, Yi Chen, Peng Wang, Yeonjoon Lee, XiaoFeng Wang, Bin Ma, Aohui Wang, Yingjun Zhang, and Wei Zou</i>	
TriggerScope: Towards Detecting Logic Bombs in Android Applications	377
<i>Yanick Fratantonio, Antonio Bianchi, William Robertson, Engin Kirda, Christopher Kruegel, and Giovanni Vigna</i>	
Inferring User Routes and Locations Using Zero-Permission Mobile Sensors	397
<i>Sashank Narain, Triet D. Vo-Huu, Kenneth Block, and Guevara Noubir</i>	
No Pardon for the Interruption: New Inference Attacks on Android Through Interrupt Timing Analysis	414
<i>Wenrui Diao, Xiangyu Liu, Zhou Li, and Kehuan Zhang</i>	
SoK: Lessons Learned from Android Security Research for Applified Software Platforms	433
<i>Yasemin Acar, Michael Backes, Sven Bugiel, Sascha Fahl, Patrick McDaniel, and Matthew Smith</i>	

Key Exchange and Certificates

Key Confirmation in Key Exchange: A Formal Treatment and Implications for TLS 1.3	452
<i>Marc Fischlin, Felix Günther, Benedikt Schmidt, and Bogdan Warinschi</i>	
Automated Analysis and Verification of TLS 1.3: 0-RTT, Resumption and Delayed Authentication	470
<i>Cas Cremers, Marko Horvat, Sam Scott, and Thyla van der Merwe</i>	
Multiple Handshakes Security of TLS 1.3 Candidates	486
<i>Xinyu Li, Jing Xu, Zhenfeng Zhang, Dengguo Feng, and Honggang Hu</i>	
Downgrade Resilience in Key-Exchange Protocols	506
<i>Karthikeyan Bhargavan, Christina Brzuska, Cédric Fournet, Matthew Green, Markulf Kohlweiss, and Santiago Zanella-Béguelin</i>	
Keeping Authorities “Honest or Bust” with Decentralized Witness Cosigning	526
<i>Ewa Syta, Iulia Tamas, Dylan Visher, David Isaac Wolinsky, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ismail Khoffi, and Bryan Ford</i>	

Learning about Privacy

Synthesizing Plausible Privacy-Preserving Location Traces	546
<i>Vincent Bindschaedler and Reza Shokri</i>	
A Method for Verifying Privacy-Type Properties: The Unbounded Case	564
<i>Lucca Hirschi, David Baelde, and Stéphanie Delaune</i>	
Distillation as a Defense to Adversarial Perturbations Against Deep Neural Networks	582
<i>Nicolas Papernot, Patrick McDaniel, Xi Wu, Somesh Jha, and Ananthram Swami</i>	
Algorithmic Transparency via Quantitative Input Influence: Theory and Experiments with Learning Systems	598
<i>Anupam Datta, Shayak Sen, and Yair Zick</i>	

Vulnerabilities

Talos: Neutralizing Vulnerabilities with Security Workarounds for Rapid Response	618
<i>Zhen Huang, Mariana D'Angelo, Dhaval Miyani, and David Lie</i>	
Security Analysis of Emerging Smart Home Applications	636
<i>Earlence Fernandes, Jaeyeon Jung, and Atul Prakash</i>	
Staying Secure and Unprepared: Understanding and Mitigating the Security Risks of Apple ZeroConf	655
<i>Xiaolong Bai, Luyi Xing, Nan Zhang, XiaoFeng Wang, Xiaojing Liao, Tongxin Li, and Shi-Min Hu</i>	

Don't Go on the Web

MitM Attack by Name Collision: Cause Analysis and Vulnerability Assessment in the New gTLD Era	675
<i>Qi Alfred Chen, Eric Osterweil, Matthew Thomas, and Z. Morley Mao</i>	
Domain-Z: 28 Registrations Later Measuring the Exploitation of Residual Trust in Domains	691
<i>Chaz Lever, Robert Walls, Yacin Nadjji, David Dagon, Patrick McDaniel, and Manos Antonakakis</i>	
Seeking Nonsense, Looking for Trouble: Efficient Promotional-Infection Detection through Semantic Inconsistency Search	707
<i>Xiaojing Liao, Kan Yuan, XiaoFeng Wang, Zhongyu Pei, Hao Yang, Jianjun Chen, Haixin Duan, Kun Du, Eihal Alowaisheq, Sumayah Alrwais, Luyi Xing, and Raheem Beyah</i>	
The Cracked Cookie Jar: HTTP Cookie Hijacking and the Exposure of Private Information	724
<i>Suphanee Sivakorn, Iasonas Polakis, and Angelos D. Keromytis</i>	

Cloak of Visibility: Detecting When Machines Browse a Different Web	743
<i>Luca Invernizzi, Kurt Thomas, Alexandros Kapravelos, Oxana Comanescu, Jean-Michel Picod, and Elie Bursztein</i>	

Applied Cryptography

Verifiable ASICs	759
<i>Riad S. Wahby, Max Howald, Siddharth Garg, Abhi Shelat, and Michael Walfish</i>	

SoK: Verifiability Notions for E-Voting Protocols	779
<i>Véronique Cortier, David Galindo, Ralf Küsters, Johannes Müller, and Tomasz Truderung</i>	

pASSWORD tYPOS and How to Correct Them Securely	799
<i>Rahul Chatterjee, Anish Athayle, Devdatta Akhawe, Ari Juels, and Thomas Ristenpart</i>	

On the Practicality of Cryptographically Enforcing Dynamic Access Control Policies in the Cloud	819
<i>William C. Garrison III, Adam Shull, Steven Myers, and Adam J. Lee</i>	

Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts	839
<i>Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou</i>	

What? You Want More?

High-Speed Inter-Domain Fault Localization	859
<i>Cristina Basescu, Yue-Hsun Lin, Haoming Zhang, and Adrian Perrig</i>	

Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints	878
<i>Pierre Laperdrix, Walter Rudametkin, and Benoit Baudry</i>	

Verena: End-to-End Integrity Protection for Web Applications	895
<i>Nikolaos Karapanos, Alexandros Filios, Raluca Ada Popa, and Srdjan Capkun</i>	

SoK: Towards Grounding Censorship Circumvention in Empiricism	914
<i>Michael Carl Tschantz, Sadia Afroz, Anonymous, and Vern Paxson</i>	

Low-Level Attacks and Defenses

A Tough Call: Mitigating Advanced Code-Reuse Attacks at the Binary Level	934
<i>Victor van der Veen, Enes Göktas, Moritz Contag, Andre Pawoloski, Xi Chen, Sanjay Rawat, Herbert Bos, Thorsten Holz, Elias Athanasopoulos, and Cristiano Giuffrida</i>	

Return to the Zombie Gadgets: Undermining Destructive Code Reads via Code Inference Attacks	954
<i>Kevin Z. Snow, Roman Rogowski, Jan Werner, Hyungjoon Koo, Fabian Monrose, and Michalis Polychronakis</i>	
Data-Oriented Programming: On the Expressiveness of Non-control Data Attacks	969
<i>Hong Hu, Shweta Shinde, Sendriu Adrian, Zheng Leong Chua, Prateek Saxena, and Zhenkai Liang</i>	
Dedup Est Machina: Memory Deduplication as an Advanced Exploitation Vector	987
<i>Erik Bosman, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida</i>	

Author Index