

2015 IEEE Symposium on Security and Privacy

(SP 2015)

**San Jose, California, USA
17-21 May 2015**



**IEEE Catalog Number: CFP15020-POD
ISBN: 978-1-4673-6950-3**

2015 IEEE Symposium on Security and Privacy

SP 2015

Table of Contents

Message from the General Chair.....	xi
Organizing Committee.....	xiv
Program Committee.....	xvi
External Reviewers.....	xviii

Hardware-Aided Security

Protecting Private Keys against Memory Disclosure Attacks Using Hardware Transactional Memory	3
<i>Le Guan, Jingqiang Lin, Bo Luo, Jiwu Jing, and Jing Wang</i>	
CHERI: A Hybrid Capability-System Architecture for Scalable Software Compartmentalization	20
<i>Robert N.M. Watson, Jonathan Woodruff, Peter G. Neumann, Simon W. Moore, Jonathan Anderson, David Chisnall, Nirav Dave, Brooks Davis, Khilan Gudka, Ben Laurie, Steven J. Murdoch, Robert Norton, Michael Roe, Stacey Son, and Munraj Vadera</i>	
VC3: Trustworthy Data Analytics in the Cloud Using SGX	38
<i>Felix Schuster, Manuel Costa, Cédric Fournet, Christos Gkantsidis, Marcus Peinado, Gloria Mainar-Ruiz, and Mark Russinovich</i>	
Using Hardware Features for Increased Debugging Transparency	55
<i>Fengwei Zhang, Kevin Leach, Angelos Stavrou, Haining Wang, and Kun Sun</i>	
Virtual Proofs of Reality and their Physical Implementation	70
<i>Ulrich Rührmair, J.L. Martinez-Hurtado, Xiaolin Xu, Christian Kraeh, Christian Hilgers, Dima Kononchuk, Jonathan J. Finley, and Wayne P. Bursleson</i>	

Cryptocurrencies and Cybercrime

The Miner's Dilemma	89
<i>Ittay Eyal</i>	

SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies	104
<i>Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten</i>	
Bitcoin over Tor isn't a Good Idea	122
<i>Alex Biryukov and Ivan Pustogarov</i>	
Every Second Counts: Quantifying the Negative Externalities of Cybercrime via Typosquatting	135
<i>Mohammad Taha Khan, Xiang Huo, Zhou Li, and Chris Kanich</i>	
Ad Injection at Scale: Assessing Deceptive Advertisement Modifications	151
<i>Kurt Thomas, Elie Bursztein, Chris Grier, Grant Ho, Nav Jagpal, Alexandros Kapravelos, Damon Mccoy, Antonio Nappa, Vern Paxson, Paul Pearce, Niels Provos, and Moheeb Abu Rajab</i>	

Protocols and Network Security

Connection-Oriented DNS to Improve Privacy and Security	171
<i>Liang Zhu, Zi Hu, John Heidemann, Duane Wessels, Allison Mankin, and Nikita Somaiya</i>	
Temporal Lensing and Its Application in Pulsing Denial-of-Service Attacks	187
<i>Ryan Rasti, Mukul Murthy, Nicholas Weaver, and Vern Paxson</i>	
Secure Track Verification	199
<i>Matthias Schäfer, Vincent Lenders, and Jens Schmitt</i>	
How Secure and Quick is QUIC? Provable Security and Performance Analyses	214
<i>Robert Lychev, Samuel Jero, Alexandra Boldyreva, and Cristina Nita-Rotaru</i>	
SoK: Secure Messaging	232
<i>Nik Unger, Sergej Dechand, Joseph Bonneau, Sascha Fahl, Henning Perl, Ian Goldberg, and Matthew Smith</i>	

Cryptographic Protocols

Geppetto: Versatile Verifiable Computation	253
<i>Craig Costello, Cédric Fournet, Jon Howell, Markulf Kohlweiss, Benjamin Kreuter, Michael Naehrig, Bryan Parno, and Samee Zahur</i>	
ADSNARK: Nearly Practical and Privacy-Preserving Proofs on Authenticated Data	271
<i>Michael Backes, Manuel Barbosa, Dario Fiore, and Raphael M. Reischuk</i>	
Secure Sampling of Public Parameters for Succinct Zero Knowledge Proofs	287
<i>Eli Ben-Sasson, Alessandro Chiesa, Matthew Green, Eran Tromer, and Madars Virza</i>	

Forward Secure Asynchronous Messaging from Puncturable Encryption	305
<i>Matthew D. Green and Ian Miers</i>	
Riposte: An Anonymous Messaging System Handling Millions of Users	321
<i>Henry Corrigan-Gibbs, Dan Boneh, and David Mazières</i>	

ORAM and Secure Multi-party Computation

Privacy and Access Control for Outsourced Personal Records	341
<i>Matteo Maffei, Giulio Malavolta, Manuel Reinert, and Dominique Schröder</i>	
OblivM: A Programming Framework for Secure Computation	359
<i>Chang Liu, Xiao Shaun Wang, Kartik Nayak, Yan Huang, and Elaine Shi</i>	
GraphSC: Parallel Secure Computation Made Easy	377
<i>Kartik Nayak, Xiao Shaun Wang, Stratis Ioannidis, Udi Weinsberg, Nina Taft, and Elaine Shi</i>	
Malicious-Client Security in Blind Seer: A Scalable Private DBMS	395
<i>Ben A. Fisc, Binh Vo, Fernando Krell, Abishek Kumarasubramanian, Vladimir Kolesnikov, Tal Malkin, and Steven M. Bellovin</i>	
TinyGarble: Highly Compressed and Scalable Sequential Garbled Circuits	411
<i>Ebrahim M. Songhori, Siam U. Hussain, Ahmad-Reza Sadeghi, Thomas Schneider, and Farinaz Koushanfar</i>	

Security du Jour

SurroundWeb: Mitigating Privacy Concerns in a 3D Web Browser	431
<i>John Vilk, David Molnar, Benjamin Livshits, Eyal Ofek, Chris Rossbach, Alexander Moshchuk, Helen J. Wang, and Ran Gal</i>	
GenoGuard: Protecting Genomic Data against Brute-Force Attacks	447
<i>Zhicong Huang, Erman Ayday, Jacques Fellay, Jean-Pierre Hubaux, and Ari Juels</i>	
Towards Making Systems Forget with Machine Unlearning	463
<i>Yinzhi Cao and Junfeng Yang</i>	
Cracking-Resistant Password Vaults Using Natural Language Encoders	481
<i>Rahul Chatterjee, Joseph Bonneau, Ari Juels, and Thomas Ristenpart</i>	
SoK: A Comprehensive Analysis of Game-Based Ballot Privacy Definitions	499
<i>David Bernhard, Véronique Cortier, David Galindo, Olivier Pereira, and Bogdan Warinschi</i>	

Protocols

Vetting SSL Usage in Applications with SSLINT	519
<i>Boyuan He, Vaibhav Rastogi, Yinzhi Cao, Yan Chen, V.N. Venkatakrishnan, Runqing Yang, and Zhenrui Zhang</i>	
A Messy State of the Union: Taming the Composite State Machines of TLS	535
<i>Benjamin Beurdouche, Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, Markulf Kohlweiss, Alfredo Pironti, Pierre-Yves Strub, and Jean Karim Zinzindohoue</i>	
Post-Quantum Key Exchange for the TLS Protocol from the Ring Learning with Errors Problem	553
<i>Joppe W. Bos, Craig Costello, Michael Naehrig, and Douglas Stebila</i>	
Security of the J-PAKE Password-Authenticated Key Exchange Protocol	571
<i>Michel Abdalla, Fabrice Benhamouda, and Philip MacKenzie</i>	

Side Channels

S\$A: A Shared Cache Attack That Works across Cores and Defies VM Sandboxing—and Its Application to AES	591
<i>Gorka Irazoqui, Thomas Eisenbarth, and Berk Sunar</i>	
Last-Level Cache Side-Channel Attacks are Practical	605
<i>Fangfei Liu, Yuval Yarom, Qian Ge, Gernot Heiser, and Ruby B. Lee</i>	
On Subnormal Floating Point and Abnormal Timing	623
<i>Marc Andryscio, David Kohlbrenner, Keaton Mowery, Ranjit Jhala, Sorin Lerner, and Hovav Shacham</i>	
Controlled-Channel Attacks: Deterministic Side Channels for Untrusted Operating Systems	640
<i>Yuanzhong Xu, Weidong Cui, and Marcus Peinado</i>	

Malware and Program Analysis

SoK: Deep Packer Inspection: A Longitudinal Study of the Complexity of Run-Time Packers	659
<i>Xabier Ugarte-Pedrero, Davide Balzarotti, Igor Santos, and Pablo G. Bringas</i>	
A Generic Approach to Automatic Deobfuscation of Executable Code	674
<i>Babak Yadegari, Brian Johannesmeyer, Ben Whitely, and Saumya Debray</i>	
The Attack of the Clones: A Study of the Impact of Shared Code on Vulnerability Patching	692
<i>Antonio Nappa, Richard Johnson, Leyla Bilge, Juan Caballero, and Tudor Dumitraş</i>	

Cross-Architecture Bug Search in Binary Executables	709
<i>Jannik Pewny, Behrad Garmany, Robert Gawlik, Christian Rossow, and Thorsten Holz</i>	
Program-Adaptive Mutational Fuzzing	725
<i>Sang Kil Cha, Maverick Woo, and David Brumley</i>	

Memory Integrity

Counterfeit Object-oriented Programming: On the Difficulty of Preventing Code Reuse Attacks in C++ Applications	745
<i>Felix Schuster, Thomas Tendyck, Christopher Liebchen, Lucas Davi, Ahmad-Reza Sadeghi, and Thorsten Holz</i>	
Readactor: Practical Code Randomization Resilient to Memory Disclosure	763
<i>Stephen Crane, Christopher Liebchen, Andrei Homescu, Lucas Davi, Per Larsen, Ahmad-Reza Sadeghi, Stefan Brunthaler, and Michael Franz</i>	
Missing the Point(er): On the Effectiveness of Code Pointer Integrity	781
<i>Isaac Evans, Sam Fingeret, Julian Gonzalez, Ulziibayar Otgonbaatar, Tiffany Tang, Howard Shrobe, Stelios Sidiroglou-Douskos, Martin Rinard, and Hamed Okhravi</i>	
Automatic Inference of Search Patterns for Taint-Style Vulnerabilities	797
<i>Fabian Yamaguchi, Alwin Maier, Hugo Gascon, and Konrad Rieck</i>	
Micro-Policies: Formally Verified, Tag-Based Security Monitors	813
<i>Arthur Azevedo de Amorim, Maxime Dénès, Nick Giannarakis, Cătălin Hrițcu, Benjamin C. Pierce, Antal Spector-Zabusky, and Andrew Tolmach</i>	

Security du Jour II

Securing Multiparty Online Services Via Certification of Symbolic Transactions	833
<i>Eric Y. Chen, Shuo Chen, Shaz Qadeer, and Rui Wang</i>	
Understanding and Monitoring Embedded Web Scripts	850
<i>Yuchen Zhou and David Evans</i>	
High System-Code Security with Low Overhead	866
<i>Jonas Wagner, Volodymyr Kuznetsov, George Candea, and Johannes Kinder</i>	
Caelus: Verifying the Consistency of Cloud Services with Battery-Powered Devices	880
<i>Beom Heyn Kim and David Lie</i>	

Android Security

Effective Real-Time Android Application Auditing	899
<i>Mingyuan Xia, Lu Gong, Yuanhao Lyu, Zhengwei Qi, and Xue Liu</i>	
Leave Me Alone: App-Level Protection against Runtime Information Gathering on Android	915
<i>Nan Zhang, Kan Yuan, Muhammad Naveed, Xiaoyong Zhou, and Xiaofeng Wang</i>	
What the App is That? Deception and Countermeasures in the Android User Interface	931
<i>Antonio Bianchi, Jacopo Corbetta, Luca Invernizzi, Yanick Fratantonio, Christopher Kruegel, and Giovanni Vigna</i>	
Author Index	949