

2011 IEEE Symposium on Security and Privacy

SP 2011

Table of Contents

Message from General Chair	ix
Message from the Program Chairs.....	xi
Symposium Organizers.....	xii
Program Committee.....	xiii
Additional Reviewers	xv

Session 1: Security of Authentication and Protection Mechanisms

Phonotactic Reconstruction of Encrypted VoIP Conversations: Hookt on Fon-iks	3
<i>Andrew M. White, Austin R. Matthews, Kevin Z. Snow, and Fabian Monroe</i>	
The Failure of Noise-Based Non-continuous Audio Captchas	19
<i>Elie Bursztein, Romain Beauxis, Hristo Paskov, Daniele Perito, Celine Fabry, and John Mitchell</i>	
Using Fingerprint Authentication to Reduce System Security: An Empirical Study	32
<i>Hugh Wimberly and Lorie M. Liebrock</i>	

Session 2: Hardware Security

Silencing Hardware Backdoors	49
<i>Adam Waksman and Simha Sethumadhavan</i>	
Defeating UCI: Building Stealthy and Malicious Hardware	64
<i>Cynthia Sturton, Matthew Hicks, David Wagner, and Samuel T. King</i>	

Session 3: Systematization of Knowledge I

Formalizing Anonymous Blacklisting Systems	81
<i>Ryan Henry and Ian Goldberg</i>	
Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices	96
<i>Michael Becher, Felix C. Freiling, Johannes Hoffmann, Thorsten Holz, Sebastian Uellenbeck, and Christopher Wolf</i>	

Session 4: Browsing Security and Privacy

Verified Security for Browser Extensions	115
<i>Arjun Guha, Matthew Fredrikson, Benjamin Livshits, and Nikhil Swamy</i>	
RePriv: Re-imagining Content Personalization and In-browser Privacy	131
<i>Matthew Fredrikson and Benjamin Livshits</i>	
I Still Know What You Visited Last Summer: Leaking Browsing History via User Interaction and Side Channel Attacks	147
<i>Zachary Weinberg, Eric Y. Chen, Pavithra Ramesh Jayaraman, and Collin Jackson</i>	

Session 5: Secure Information Flow and Information Policies

Verification of Information Flow and Access Control Policies with Dependent Types	165
<i>Aleksandar Nanevski, Anindya Banerjee, and Deepak Garg</i>	
Inference of Expressive Declassification Policies	180
<i>Jeffrey A. Vaughan and Stephen Chong</i>	
The Complexity of Intransitive Noninterference	196
<i>Sebastian Eggert, Ron van der Meyden, Henning Schnoor, and Thomas Wilke</i>	
SCION: Scalability, Control, and Isolation on Next-Generation Networks	212
<i>Xin Zhang, Hsu-Chun Hsiao, Geoffrey Hasker, Haowen Chan, Adrian Perrig, and David G. Andersen</i>	

Session 6: Privacy and Social Networks

"You Might Also Like:" Privacy Risks of Collaborative Filtering	231
<i>Joseph A. Calandrino, Ann Kilzer, Arvind Narayanan, Edward W. Felten, and Vitaly Shmatikov</i>	
Quantifying Location Privacy	247
<i>Reza Shokri, George Theodorakopoulos, Jean-Yves Le Boudec, and Jean-Pierre Hubaux</i>	
Preventing Sybil Attacks by Privilege Attenuation: A Design Principle for Social Network Systems	263
<i>Philip W.L. Fong</i>	

Session 7: Virtualization and Trusted Computing

PRISM: Program Replication and Integration for Seamless MILS	281
<i>Chris Owen, Duncan Grove, Tristan Newby, Alex Murray, Chris North, and Michael Pope</i>	
Virtuoso: Narrowing the Semantic Gap in Virtual Machine Introspection	297
<i>Brendan Dolan-Gavitt, Tim Leek, Michael Zhivich, Jonathon Giffin, and Wenke Lee</i>	
HomeAlone: Co-residency Detection in the Cloud via Side-Channel Analysis	313
<i>Yinqian Zhang, Ari Juels, Alina Oprea, and Michael K. Reiter</i>	

TxBBox: Building Secure, Efficient Sandboxes with System Transactions	329
<i>Suman Jana, Donald E. Porter, and Vitaly Shmatikov</i>	

Session 8: Program Security Analysis

Differential Slicing: Identifying Causal Execution Differences for Security Applications	347
<i>Noah M. Johnson, Juan Caballero, Kevin Zhijie Chen, Stephen McCamant, Pongsin Poosankam, Daniel Reynaud, and Dawn Song</i>	
Automated Analysis of Security-Critical JavaScript APIs	363
<i>Ankur Taly, Úlfar Erlingsson, John C. Mitchell, Mark S. Miller, and Jasvir Nagra</i>	
Memoir: Practical State Continuity for Protected Modules	379
<i>Bryan Parno, Jacob R. Lorch, John R. Douceur, James Mickens, and Jonathan M. McCune</i>	

Session 9: Systematization of Knowledge II

A Formalization of the Security Features of Physical Functions	397
<i>Frederik Armknecht, Roel Maes, Ahmad-Reza Sadeghi, François-Xavier Standaert, and Christian Wachsmann</i>	
Timing- and Termination-Sensitive Secure Information Flow: Exploring a New Approach	413
<i>Vineeth Kashyap, Ben Wiedermann, and Ben Hardekopf</i>	

Session 10: Underground Economy/Malware

Click Trajectories: End-to-End Analysis of the Spam Value Chain	431
<i>Kirill Levchenko, Andreas Pitsillidis, Neha Chachra, Brandon Enright, Márk Félegyházi, Chris Grier, Tristan Halvorson, Chris Kanich, Christian Kreibich, He Liu, Damon McCoy, Nicholas Weaver, Vern Paxson, Geoffrey M. Voelker, and Stefan Savage</i>	
Design and Evaluation of a Real-Time URL Spam Filtering Service	447
<i>Kurt Thomas, Chris Grier, Justin Ma, Vern Paxson, and Dawn Song</i>	

Session 11: Vulnerability Analysis

How to Shop for Free Online—Security Analysis of Cashier-as-a-Service Based Web Stores	465
<i>Rui Wang, Shuo Chen, XiaoFeng Wang, and Shaz Qadeer</i>	
Cryptography in the Web: The Case of Cryptographic Design Flaws in ASP.NET	481
<i>Thai Duong and Julian Rizzo</i>	
Cache Games—Bringing Access-Based Cache Attacks on AES to Practice	490
<i>David Gullasch, Endre Bangerter, and Stephan Krenn</i>	
OpenConflict: Preventing Real Time Map Hacks in Online Games	506
<i>Elie Bursztein, Mike Hamburg, Jocelyn Lagarenne, and Dan Boneh</i>	

Session 12: Anonymity and Voting

Extending Nymble-like Systems	523
<i>Ryan Henry and Ian Goldberg</i>	
Verifiability, Privacy, and Coercion-Resistance: New Insights from a Case Study	538
<i>Ralf Küesters, Tomasz Truderung, and Andreas Vogt</i>	
Author Index	554