2011 IEEE Symposium on Security and Privacy

(SP 2011)

Oakland, California, USA
22 – 25 May 2011

IEEE Catalog Number:	CFP11020-PRT
ISBN:	978-1-4577-0147-4

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
Andrew M. White, Austin R. Matthews, Kevin Z. Snow, and Fabian Monrose

The Failure of Noise-Based Non-continuous Audio Captchas 19
Elie Bursztein, Romain Beauxis, Hristo Paskov, Daniele Perito, Celine Fabry, and John Mitchell

Using Fingerprint Authentication to Reduce System Security: An Empirical Study 32
Hugh Wimberly and Lorie M. Liebrock

Session 2: Hardware Security

Silencing Hardware Backdoors 49
Adam Waksman and Simha Sethumadhavan

Defeating UCI: Building Stealthy and Malicious Hardware 64
Cynthia Sturton, Matthew Hicks, David Wagner, and Samuel T. King

Session 3: Systematization of Knowledge I

Formalizing Anonymous Blacklisting Systems 81
Ryan Henry and Ian Goldberg

Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices 96
Michael Becher, Felix C. Freiling, Johannes Hoffmann, Thorsten Holz, Sebastian Uellenbeck, and Christopher Wolf

Session 4: Browsing Security and Privacy

Verified Security for Browser Extensions 115
Arjun Guha, Matthew Fredrikson, Benjamin Livshits, and Nikhil Swamy

RePriv: Re-imagining Content Personalization and In-browser Privacy 131
Matthew Fredrikson and Benjamin Livshits

I Still Know What You Visited Last Summer: Leaking Browsing History via User Interaction and Side Channel Attacks 147
Zachary Weinberg, Eric Y. Chen, Pavithra Ramesh Jayaraman, and Collin Jackson

Session 5: Secure Information Flow and Information Policies

Verification of Information Flow and Access Control Policies with Dependent Types 165
Aleksandar Nanevski, Anindya Banerjee, and Deepak Garg

Inference of Expressive Declassification Policies 180
Jeffrey A. Vaughan and Stephen Chong

The Complexity of Intransitive Noninterference 196
Sebastian Eggert, Ron van der Meyden, Henning Schnoor, and Thomas Wilke

SCION: Scalability, Control, and Isolation on Next-Generation Networks 212
Xin Zhang, Hsu-Chun Hsiao, Geoffrey Hasker, Haowen Chan, Adrian Perrig, and David G. Andersen

Session 6: Privacy and Social Networks

"You Might Also Like:" Privacy Risks of Collaborative Filtering 231
Joseph A. Calandrino, Ann Kilzer, Arvind Narayanan, Edward W. Felten, and Vitaly Shmatikov

Quantifying Location Privacy 247
Reza Shokri, George Theodorakopoulos, Jean-Yves Le Boudec, and Jean-Pierre Hubaux

Preventing Sybil Attacks by Privilege Attenuation: A Design Principle for Social Network Systems 263
Philip W.L. Fong

Session 7: Virtualization and Trusted Computing

PRISM: Program Replication and Integration for Seamless MILS 281
Chris Owen, Duncan Grove, Tristan Newby, Alex Murray, Chris North, and Michael Pope

Virtuoso: Narrowing the Semantic Gap in Virtual Machine Introspection 297
Brendan Dolan-Gavitt, Tim Leek, Michael Zhivich, Jonathon Giffin, and Wenke Lee

HomeAlone: Co-residency Detection in the Cloud via Side-Channel Analysis 313
Yinqian Zhang, Ari Juels, Alina Oprea, and Michael K. Reiter

TxBox: Building Secure, Efficient Sandboxes with System Transactions 329
Suman Jana, Donald E. Porter, and Vitaly Shmatikov

Session 8: Program Security Analysis

Differential Slicing: Identifying Causal Execution Differences for Security Applications 347
Noah M. Johnson, Juan Caballero, Kevin Zhijie Chen, Stephen McCamant, Pongsin Poosankam, Daniel Reynaud, and Dawn Song

Automated Analysis of Security-Critical JavaScript APIs 363
Ankur Taly, Úlfar Erlingsson, John C. Mitchell, Mark S. Miller, and Jasvir Nagra

Memoir: Practical State Continuity for Protected Modules 379
Bryan Parno, Jacob R. Lorch, John R. Douceur, James Mickens, and Jonathan M. McCune

Session 9: Systematization of Knowledge II

A Formalization of the Security Features of Physical Functions 397
Frederik Armknecht, Roel Maes, Ahmad-Reza Sadeghi, François-Xavier Standaert, and Christian Wachsmann

Timing- and Termination-Sensitive Secure Information Flow: Exploring a New Approach 413
Vineeth Kashyap, Ben Wiedermann, and Ben Hardekopf

Session 10: Underground Economy/Malware

Click Trajectories: End-to-End Analysis of the Spam Value Chain 431
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

Design and Evaluation of a Real-Time URL Spam Filtering Service 447
Kurt Thomas, Chris Grier, Justin Ma, Vern Paxson, and Dawn Song

Session 11: Vulnerability Analysis

How to Shop for Free Online—Security Analysis of Cashier-as-a-Service Based Web Stores 465
Rui Wang, Shuo Chen, XiaoFeng Wang, and Shaz Qadeer

Cryptography in the Web: The Case of Cryptographic Design Flaws in ASP.NET 481
Thai Duong and Juliano Rizzo

Cache Games—Bringing Access-Based Cache Attacks on AES to Practice 490
David Gullasch, Endre Bangerter, and Stephan Krenn

OpenConflict: Preventing Real Time Map Hacks in Online Games 506
Elie Bursztein, Mike Hamburg, Jocelyn Lagarenne, and Dan Boneh

Session 12: Anonymity and Voting

Extending Nymble-like Systems 523
Ryan Henry and Ian Goldberg

Verifiability, Privacy, and Coercion-Resistance: New Insights from a Case Study 538
Ralf Küesters, Tomasz Truderung, and Andreas Vogt

Author Index 554