

2012 IEEE Symposium on Security and Privacy

(SP 2012)

**San Francisco, California, USA
20 – 23 May 2012**



IEEE Catalog Number: CFP12020-PRT
ISBN: 978-1-4673-1244-8

2012 IEEE Symposium on Security and Privacy

S&P 2012

Table of Contents

Message from the General Chair.....	ix
Message from the Program Chairs.....	xi
Organizing Committee.....	xii
Program Committee.....	xiii
Reviewers	xv

Session 1: System Security

A Framework to Eliminate Backdoors from Response-Computable Authentication	3
<i>Shuaifu Dai, Tao Wei, Chao Zhang, Tielei Wang, Yu Ding, Zhenkai Liang, and Wei Zou</i>	
Safe Loading - A Foundation for Secure Execution of Untrusted Programs	18
<i>Mathias Payer, Tobias Hartmann, and Thomas R. Gross</i>	
Flash Memory for Ubiquitous Hardware Security Functions: True Random Number Generation and Device Fingerprints	33
<i>Yinglei Wang, Wing-kei Yu, Shuo Wu, Greg Malysa, G. Edward Suh, and Edwin C. Kan</i>	
ReDeBug: Finding Unpatched Code Clones in Entire OS Distributions	48
<i>Jiyong Jang, Abeer Agrawal, and David Brumley</i>	

Session 2: Malware

Prudent Practices for Designing Malware Experiments: Status Quo and Outlook	65
<i>Christian Rossow, Christian J. Dietrich, Chris Grier, Christian Kreibich, Vern Paxson, Norbert Pohlmann, Herbert Bos, and Maarten van Steen</i>	
Abusing File Processing in Malware Detectors for Fun and Profit	80
<i>Suman Jana and Vitaly Shmatikov</i>	
Dissecting Android Malware: Characterization and Evolution	95
<i>Yajin Zhou and Xuxian Jiang</i>	

Session 3: Attacks 1

Distance Hijacking Attacks on Distance Bounding Protocols	113
<i>Cas Cremers, Kasper B. Rasmussen, Benedikt Schmidt, and Srdjan Čapkun</i>	
Don't Trust Satellite Phones: A Security Analysis of Two Satphone Standards	128
<i>Benedikt Driessen, Ralf Hund, Carsten Willems, Christof Paar, and Thorsten Holz</i>	
Memento: Learning Secrets from Process Footprints	143
<i>Suman Jana and Vitaly Shmatikov</i>	

Session 4: Foundations

Foundations of Logic-Based Trust Management	161
<i>Moritz Y. Becker, Alessandra Russo, and Nik Sultana</i>	
Formalizing and Enforcing Purpose Restrictions in Privacy Policies	176
<i>Michael Carl Tschantz, Anupam Datta, and Jeannette M. Wing</i>	
Sharing Mobile Code Securely with Information Flow Control	191
<i>Owen Arden, Michael D. George, Jed Liu, K. Vikram, Aslan Askarov, and Andrew C. Myers</i>	

Session 5: Access Control and Attestation

The Psychology of Security for the Home Computer User	209
<i>Adele E. Howe, Indrajit Ray, Mark Roberts, Malgorzata Urbanska, and Zinta Byrne</i>	
User-Driven Access Control: Rethinking Permission Granting in Modern Operating Systems	224
<i>Franziska Roesner, Tadayoshi Kohno, Alexander Moshchuk, Bryan Parno, Helen J. Wang, and Crispin Cowan</i>	
New Results for Timing-Based Attestation	239
<i>Xeno Kovah, Corey Kallenberg, Chris Weathers, Amy Herzog, Matthew Albin, and John Butterworth</i>	

Session 6: Privacy

ObliviAd: Provably Secure and Practical Online Behavioral Advertising	257
<i>Michael Backes, Aniket Kate, Matteo Maffei, and Kim Pecina</i>	
Quid-Pro-Quo-tocols: Strengthening Semi-honest Protocols with Dual Execution	272
<i>Yan Huang, Jonathan Katz, and David Evans</i>	
Hummingbird: Privacy at the Time of Twitter	285
<i>Emiliano De Cristofaro, Claudio Soriente, Gene Tsudik, and Andrew Williams</i>	

On the Feasibility of Internet-Scale Author Identification	300
<i>Arvind Narayanan, Hristo Paskov, Neil Zhenqiang Gong, John Bethencourt, Emil Stefanov, Eui Chul Richard Shin, and Dawn Song</i>	

Session 7: Network Security

Secure and Scalable Fault Localization under Dynamic Traffic Patterns	317
<i>Xin Zhang, Chang Lan, and Adrian Perrig</i>	
Peek-a-Boo, I Still See You: Why Efficient Traffic Analysis Countermeasures Fail	332
<i>Kevin P. Dyer, Scott E. Coull, Thomas Ristenpart, and Thomas Shrimpton</i>	
Off-path TCP Sequence Number Inference Attack - How Firewall Middleboxes Reduce Security	347
<i>Zhiyun Qian and Z. Morley Mao</i>	

Session 8: Attacks 2

Signing Me onto Your Accounts through Facebook and Google: A Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services	365
<i>Rui Wang, Shuo Chen, and XiaoFeng Wang</i>	
Unleashing Mayhem on Binary Code	380
<i>Sang Kil Cha, Thanassis Avgerinos, Alexandre Rebert, and David Brumley</i>	
Clash Attacks on the Verifiability of E-Voting Systems	395
<i>Ralf Küsters, Tomasz Truderung, and Andreas Vogt</i>	

Session 9: Web Security

Third-Party Web Tracking: Policy and Technology	413
<i>Jonathan R. Mayer and John C. Mitchell</i>	
EvilSeed: A Guided Approach to Finding Malicious Web Pages	428
<i>Luca Invernizzi and Paolo Milani Comparetti</i>	
Rozzle: De-cloaking Internet Malware	443
<i>Clemens Kolbitsch, Benjamin Livshits, Benjamin Zorn, and Christian Seifert</i>	

Session 10: Privacy and Anonymity

Detecting Hoaxes, Frauds, and Deception in Writing Style Online	461
<i>Sadia Afroz, Michael Brennan, and Rachel Greenstadt</i>	
LASTor: A Low-Latency AS-Aware Tor Client	476
<i>Masoud Akhoondi, Curtis Yu, and Harsha V. Madhyastha</i>	
OB-PWS: Obfuscation-Based Private Web Search	491
<i>Ero Balsa, Carmela Troncoso, and Claudia Diaz</i>	

LAP: Lightweight Anonymity and Privacy	506
<i>Hsu-Chun Hsiao, Tiffany Hyun-Jin Kim, Adrian Perrig, Akira Yamada, Samuel C. Nelson, Marco Gruteser, and Wei Meng</i>	

Session 11: Passwords

Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms	523
<i>Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Julio López</i>	
The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords	538
<i>Joseph Bonneau</i>	
The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes	553
<i>Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano</i>	

Session 12: System Security

ILR: Where'd My Gadgets Go?	571
<i>Jason Hiser, Anh Nguyen-Tuong, Michele Co, Matthew Hall, and Jack W. Davidson</i>	
Space Traveling across VM: Automatically Bridging the Semantic Gap in Virtual Machine Introspection via Online Kernel Data Redirection	586
<i>Yangchun Fu and Zhiqiang Lin</i>	
Smashing the Gadgets: Hindering Return-Oriented Programming Using In-place Code Randomization	601
<i>Vasilis Pappas, Michalis Polychronakis, and Angelos D. Keromytis</i>	
Building Verifiable Trusted Path on Commodity x86 Computers	616
<i>Zongwei Zhou, Virgil D. Gligor, James Newsome, and Jonathan M. McCune</i>	
Author Index	631