

# **2009 IEEE Symposium on Security and Privacy**

**(SP 2009)**

**Oakland, California, USA  
17-20 May 2009**



**IEEE Catalog Number: CFP09020-PRT  
ISBN: 978-1-4244-3982-9**

# 2009 30th IEEE Symposium on Security and Privacy

---

**SP 2009**

## Table of Contents

### Conference Information

---

#### Session 1: Attacks and Defenses

Wirelessly Pickpocketing a Mifare Classic Card .....	3
<i>Flavio D. Garcia, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur</i>	
Plaintext Recovery Attacks against SSH .....	16
<i>Martin R. Albrecht, Kenneth G. Paterson, and Gaven J. Watson</i>	
Exploiting Unix File-System Races via Algorithmic Complexity Attacks .....	27
<i>Xiang Cai, Yuwei Gui, and Rob Johnson</i>	

#### Session 2: Information Security

Practical Mitigations for Timing-Based Side-Channel Attacks on Modern x86 Processors .....	45
<i>Bart Coppens, Ingrid Verbauwhede, Koen De Bosschere, and Bjorn De Sutter</i>	
Noninterference for a Practical DIFC-Based Operating System .....	61
<i>Maxwell Krohn and Eran Tromer</i>	

#### Session 3: Malicious Code

Native Client: A Sandbox for Portable, Untrusted x86 Native Code .....	79
<i>Bennet Yee, David Sehr, Gregory Dardyk, J. Bradley Chen, Robert Muth, Tavis Ormandy, Shiki Okasaka, Neha Narula, and Nicholas Fullagar</i>	
Automatic Reverse Engineering of Malware Emulators .....	94
<i>Monirul Sharif, Andrea Lanzi, Jonathon Giffin, and Wenke Lee</i>	
Prospex: Protocol Specification Extraction .....	110
<i>Paolo Milani Comparetti, Gilbert Wondracek, Christopher Kruegel, and Engin Kirda</i>	

## Session 4: Information Leaks

Quantifying Information Leaks in Outbound Web Traffic .....	129
<i>Kevin Borders and Atul Prakash</i>	
Automatic Discovery and Quantification of Information Leaks .....	141
<i>Michael Backes, Boris Köpf, and Andrey Rybalchenko</i>	
CLAMP: Practical Prevention of Large-Scale Data Leaks .....	154
<i>Bryan Parno, Jonathan M. McCune, Dan Wendlandt, David G. Andersen, and Adrian Perrig</i>	

## Session 5: Privacy

De-anonymizing Social Networks .....	173
<i>Arvind Narayanan and Vitaly Shmatikov</i>	
Privacy Weaknesses in Biometric Sketches .....	188
<i>Koen Simoens, Pim Tuyls, and Bart Preneel</i>	
The Mastermind Attack on Genomic Data .....	204
<i>Michael T. Goodrich</i>	

## Session 6: Formal Foundations

A Logic of Secure Systems and its Application to Trusted Computing .....	221
<i>Anupam Datta, Jason Franklin, Deepak Garg, and Dilsun Kaynar</i>	
Formally Certifying the Security of Digital Signature Schemes .....	237
<i>Santiago Zanella-Béguelin, Gilles Barthe, Benjamin Grégoire, and Federico Olmedo</i>	
An Epistemic Approach to Coercion-Resistance for Electronic Voting Protocols .....	251
<i>Ralf Kuesters and Tomasz Truderung</i>	

## Session 7: Network Security

Sphinx: A Compact and Provably Secure Mix Format .....	269
<i>George Danezis and Ian Goldberg</i>	
DSybil: Optimal Sybil-Resistance for Recommendation Systems .....	283
<i>Haifeng Yu, Chenwei Shi, Michael Kaminsky, Phillip B. Gibbons, and Feng Xiao</i>	

## Session 8: Physical Security

Fingerprinting Blank Paper Using Commodity Scanners .....	301
<i>William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J. Alex Halderman, and Edward W. Felten</i>	
Tempest in a Teapot: Compromising Reflections Revisited .....	315
<i>Michael Backes, Tongbo Chen, Markus Duermuth, Hendrik P.A. Lensch, and Martin Welk</i>	

## Session 9: Web Security

Blueprint: Robust Prevention of Cross-site Scripting Attacks for Existing Browsers .....	331
<i>Mike Ter Louw and V.N. Venkatakrisnan</i>	
Pretty-Bad-Proxy: An Overlooked Adversary in Browsers' HTTPS Deployments .....	347
<i>Shuo Chen, Ziqing Mao, Yi-Min Wang, and Ming Zhang</i>	
Secure Content Sniffing for Web Browsers, or How to Stop Papers from Reviewing Themselves .....	360
<i>Adam Barth, Juan Caballero, and Dawn Song</i>	

## Session 10: Humans and Secrets

It's No Secret. Measuring the Security and Reliability of Authentication via "Secret" Questions .....	375
<i>Stuart Schechter, A.J. Bernheim Brush, and Serge Egelman</i>	
Password Cracking Using Probabilistic Context-Free Grammars .....	391
<i>Matt Weir, Sudhir Aggarwal, Breno de Medeiros, and Bill Glodek</i>	

## Author Index