17th USENIX Security Symposium
July 28–August 1, 2008
San Jose, CA, USA

Index of Authors . . . vi

Message from the Program Chair . . . vii

Wednesday, July 30

Web Security

All Your iFRAMEs Point to Us . . . 1
Niels Provos and Panayiotis Mavrommatis, Google Inc.; Moheeb Abu Rajab and Fabian Monrose, Johns Hopkins University

Securing Frame Communication in Browsers . . . 17
Adam Barth, Collin Jackson, and John C. Mitchell, Stanford University

Automatic Generation of XSS and SQL Injection Attacks with Goal-Directed Model Checking . . . 31
Michael Martin and Monica S. Lam, Stanford University

Cryptographic Keys

Lest We Remember: Cold Boot Attacks on Encryption Keys . . . 45
J. Alex Halderman, Princeton University; Seth D. Schoen, Electronic Frontier Foundation; Nadia Heninger and William Clarkson, Princeton University; William Paul, Wind River Systems; Joseph A. Calandrino and Ariel J. Feldman, Princeton University; Jacob Appelbaum; Edward W. Felten, Princeton University

The Practical Subtleties of Biometric Key Generation . . . 61
Lucas Ballard and Seny Kamara, The Johns Hopkins University; Michael K. Reiter, University of North Carolina at Chapel Hill

Unidirectional Key Distribution Across Time and Space with Applications to RFID Security . . . 75
Ari Juels, RSA Laboratories; Ravikanth Pappu, ThingMagic Inc; Bryan Parno, Carnegie Mellon University

Network Defenses

CloudAV: N-Version Antivirus in the Network Cloud . . . 91
Jon Oberheide, Evan Cooke, and Farnam Jahanian, University of Michigan

Highly Predictive Blacklisting . . . 107
Jian Zhang and Phillip Porras, SRI International; Johannes Ullrich, SANS Institute

Proactive Surge Protection: A Defense Mechanism for Bandwidth-Based Attacks . . . 123
Jerry Chou and Bill Lin, University of California, San Diego; Subhabrata Sen and Oliver Spatscheck, AT&T Labs—Research

Thursday, July 31

Botnet Detection

BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection . . 139
Guofei Gu, Georgia Institute of Technology; Roberto Perdisci, Damballa, Inc.; Junjie Zhang and Wenke Lee, Georgia Institute of Technology

Measurement and Classification of Humans and Bots in Internet Chat 155
Steven Gianvecchio, Mengjun Xie, Zhengyu Wu, and Haining Wang, The College of William and Mary

To Catch a Predator: A Natural Language Approach for Eliciting Malicious Payloads 171
Sam Small, Joshua Mason, and Fabian Monrose, Johns Hopkins University; Niels Provos, Google Inc.; Adam Stubblefield, Johns Hopkins University

Hardware and Security

Reverse-Engineering a Cryptographic RFID Tag 185
Karsten Nohl and David Evans, University of Virginia; Starbug and Henryk Plötz, Chaos Computer Club, Berlin

Practical Symmetric Key Cryptography on Modern Graphics Hardware 195
Owen Harrison and John Waldron, Trinity College Dublin

An Improved Clock-skew Measurement Technique for Revealing Hidden Services 211
Sebastian Zander, Swinburne University of Technology, Australia; Steven J. Murdoch, Computer Laboratory, University of Cambridge

Systems Security

NetAuth: Supporting User-Based Network Services. 227
Manigandan Radhakrishnan and Jon A. Solworth, University of Illinois at Chicago

Hypervisor Support for Identifying Covertly Executing Binaries 243
Lionel Litty, H. Andrés Lagar-Cavilla, and David Lie, University of Toronto

Selective Versioning in a Secure Disk System. 259
Swaminathan Sundararaman, Gopalan Sivathanu, and Erez Zadok, Stony Brook University

Privacy

Privacy-Preserving Location Tracking of Lost or Stolen Devices: Cryptographic Techniques and Replacing Trusted Third Parties with DHTs 275
Thomas Ristenpart, University of California, San Diego; Gabriel Maganis, Arvind Krishnamurthy, and Tadayoshi Kohno, University of Washington

Panalyst: Privacy-Aware Remote Error Analysis on Commodity Software 291
Rui Wang and XiaoFeng Wang, Indiana University at Bloomington; Zhuowei Li, Center for Software Excellence, Microsoft

Multi-flow Attacks Against Network Flow Watermarking Schemes 307
Negar Kiyavash, Amir Houmansadr, and Nikita Borisov, University of Illinois at Urbana-Champaign

Friday, August 1

Voting and Trusted Systems

Verifying Compliance of Trusted Programs 321
Sandra Rueda, Dave King, and Trent Jaeger, The Pennsylvania State University

Helios: Web-based Open-Audit Voting 335
Ben Adida, Harvard University

VoteBox: A Tamper-evident, Verifiable Electronic Voting System 349
Daniel Sandler, Kyle Derr, and Dan S. Wallach, Rice University

Software Security

An Empirical Security Study of the Native Code in the JDK 365
Gang Tan and Jason Croft, Boston College

AutoISES: *Auto*matically *I*nferring *Se*curity *S*pecification and Detecting Violations 379
Lin Tan, University of Illinois, Urbana-Champaign; Xiaolan Zhang, IBM T.J. Watson Research Center; Xiao Ma, University of Illinois, Urbana-Champaign, and Pattern Insight Inc.; Weiwei Xiong, University of Illinois, Urbana-Champaign; Yuanyuan Zhou, University of Illinois, Urbana-Champaign, and Pattern Insight Inc.

Real-World Buffer Overflow Protection for Userspace and Kernelspace 395
Michael Dalton, Hari Kannan, and Christos Kozyrakis, Stanford University