Proceedings

2006 IEEE Symposium on Security and Privacy
(S&P 2006)

21-24 May 2006

Berkeley/Oakland, California

Sponsored by

IBM Corporation

IEEE
COMPUTER
SOCIETY

IEEE

Los Alamitos, California
Washington • Tokyo

Copyright © 2006 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved.

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries may photocopy beyond the limits of US copyright law, for private use of patrons, those articles in this volume that carry a code at the bottom of the first page, provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

Other copying, reprint, or republication requests should be addressed to: IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, P.O. Box 133, Piscataway, NJ 08855-1331.

The papers in this book comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interests of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors, the IEEE Computer Society, or the Institute of Electrical and Electronics Engineers, Inc.

IEEE Computer Society Order Number P2574
ISBN-13: 978-0-7695-2574-7
ISBN-10: 0-7695-2574-1
ISSN 1081-6011

Additional copies may be ordered from:

IEEE Computer Society
Customer Service Center
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314
Tel: + 1 800 272 6657
Fax: + 1 714 821 4641
http://computer.org/cspress
csbooks@computer.org

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1 732 981 0060
Fax: + 1 732 981 9667
http://shop.ieee.org/store/
customer-service@ieee.org

IEEE Computer Society
Asia/Pacific Office
Watanabe Bldg., 1-4-2
Minami-Aoyama
Minato-ku, Tokyo 107-0062
JAPAN
Tel: + 81 3 3408 3118
Fax: + 81 3 3408 3553
tokyo.ofc@computer.org

Individual paper REPRINTS may be ordered at: reprints@computer.org

Editorial production by Bob Werner

Cover art production by Joseph Daigle/Studio Productions

Printed in the United States of America by The Printing House

IEEE
COMPUTER
SOCIETY

IEEE

IEEE Computer Society
Conference Publishing Services
http://www.computer.org/proceedings/

Table of Contents: S&P 2006

2006 IEEE Symposium on Security and Privacy

Message from the Program Chairs ______ **viii**
Conference Organizers ______ **ix**
Program Committee ______ **ix**
External Reviewers ______ **x**

Session: Signature Generation

Towards Automatic Generation of Vulnerability-Based Signatures ______ 2
David Brumley, James Newsome, Dawn Song, Hao Wang, and Somesh Jha

Misleading Worm Signature Generators Using Deliberate Noise Injection ______ 17
Roberto Perdisci, David Dagon, Wenke Lee, Prahlad Fogla, and Monirul Sharif

Hamsa: Fast Signature Generation for Zero-day Polymorphic Worms with Provable Attack Resilience ______ 32
Zhichun Li, Manan Sanghi, Yan Chen, Ming-Yang Kao, and Brian Chavez

Session: Detection

Dataflow Anomaly Detection ______ 48
Sandeep Bhatkar, Abhishek Chaturvedi, and R. Sekar

A Framework for the Evaluation of Intrusion Detection Systems ______ 63
Alvaro A. Cárdenas, Karl Seamon, and John S. Baras

Siren: Catching Evasive Malware (Short Paper) ______ 78
Kevin Borders, Xin Zhao, and Atul Prakash

Session: Privacy

Fundamental Limits on the Anonymity Provided by the MIX Technique ______ 86
Dakshi Agrawal, Dogan Kesdogan, Vinh Pham, and Dieter Rautenbach

Locating Hidden Servers ______ 100
Lasse Øverlier and Paul Syverson

Practical Inference Control for Data Cubes (Extended Abstract) ______ 115
Yingjiu Li, Haibing Lu, and Robert H. Deng

Deterring Voluntary Trace Disclosure in Re-encryption Mix Networks ______ 121
Philippe Golle, XiaoFeng Wang, Markus Jakobsson, and Alex Tsow

New Constructions and Practical Applications for Private Stream Searching (Extended Abstract) ______ 132
John Bethencourt, Dawn Song, and Brent Waters

Session: Formal Methods

A Computationally Sound Mechanized Prover for Security Protocols ________ 140
Bruno Blanchet

A Logic for Constraint-Based Security Protocol Analysis ________ 155
Ricardo Corin, Ari Saptawijaya, and Sandro Etalle

Simulatable Security and Polynominally Bounded Concurrent Composability ________ 169
Dennis Hofheinz and Dominique Unruh

Session: Analyzing and Enforcing Policy

Privacy and Contextual Integrity: Framework and Applications ________ 184
Adam Barth, Anupam Datta, John C. Mitchell, and Helen Nissenbaum

FIREMAN: A Toolkit for FIREwall Modeling and ANalysis ________ 199
Lihua Yuan, Jianning Mai, Zhendong Su, Hao Chen, Chen-Nee Chuah, and Prasant Mohapatra

Retrofitting Legacy Code for Authorization Policy Enforcement ________ 214
Vinod Ganapathy, Trent Jaeger, and Somesh Jha

Session: Analyzing Code

Deriving an Information Flow Checker and Certifying Compiler for Java ________ 230
Gilles Barthe, David A. Naumann, and Tamara Rezk

Automatically Generating Malicious Disks Using Symbolic Execution ________ 243
Paul Twohey, Junfeng Yang, Can Sar, Cristian Cadar, and Dawson Engler

Pixy: A Static Analysis Tool for Detecting Web Application Vulnerabilities (Short Paper) ________ 258
Nenad Jovanovic, Christopher Kruegel, and Engin Kirda

Cobra: Fine-grained Malware Analysis Using Stealth Localized-Executions ________ 264
Amit Vasudevan and Ramesh Yerraballi

Session: Authentication

Integrity (*I*) Codes: Message Integrity Protection and Authentication over Insecure Channels ________ 280
Mario Čagalj, Srdjan Čapkun, Ramkumar Rengaswamy,
Ilias Tsigkogiannis, Mani Srivastava, and Jean-Pierre Hubaux

Cognitive Authentication Schemes Safe Against Spyware (Short Paper) ________ 295
Daphna Weinshall

Cache Cookies for Browser Authentication (Extended Abstract) ________ 301
Ari Juels, Markus Jakobsson, and Tom N. Jagatic

Secure Device Pairing Based on a Visual Channel (Short Paper) ________ 306
Nitesh Saxena, Jan-Erik Ekberg, Kari Kostiainen, and N. Asokan

Session: Attacks

SubVirt: Implementing Malware with Virtual Machines ____ 314
Samuel T. King, Peter M. Chen, Yi-Min Wang,
Chad Verbowski, Helen J. Wang, and Jacob R. Lorch

Practical Attacks on Proximity Identification Systems (Short Paper) ____ 328
Gerhard P. Hancke

On the Secrecy of Timing-Based Active Watermarking Trace-Back Techniques ____ 334
Pai Peng, Peng Ning, and Douglas S. Reeves

Session: Systems

A Safety-Oriented Platform for Web Applications ____ 350
Richard S. Cox, Jacob Gorm Hansen, Steven D. Gribble, and Henry M. Levy

Tamper-Evident, History-Independent, Subliminal-Free Data Structures on
PROM Storage -or- How to Store Ballots on a Voting Machine (Extended Abstract) ____ 365
David Molnar, Tadayoshi Kohno, Naveen Sastry, and David Wagner

Analysis of the Linux Random Number Generator ____ 371
Zvi Gutterman, Benny Pinkas, and Tzachy Reinman

The Final Nail in WEP's Coffin ____ 386
Andrea Bittau, Mark Handley, and Joshua Lackey

Author Index ____ 401