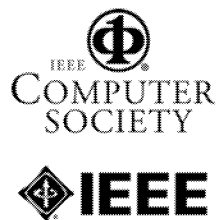


Proceedings of

22nd Annual Computer Security Applications Conference

11-15 December 2006, Miami Beach, Florida, USA



Los Alamitos, California

Washington • Tokyo

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 P2716

ISBN 0-7695-2716-7

ISBN 978-0-7695-2716-1

ISSN Number 1063-9527

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](http://shop.ieee.org/store/customer-service@ieee.org)

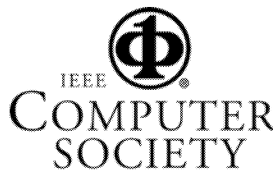
IEEE Computer Society
Asia/Pacific Office
Watanabe Bldg., 1-4-2
Minami-Aoyama
Minato-ku, Tokyo 107-0062
JAPAN
Tel: + 81 3 3408 3118
Fax: + 81 3 3408 3553
tokyo.ofc@computer.org

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

Editorial production by Bob Werner

Cover art production by Joe Daigle/Studio Productions

Printed in the United States of America by The Printing House



IEEE Computer Society

Conference Publishing Services

<http://www.computer.org/proceedings/>

Table of Contents: ACSAC 2006

22nd Annual Computer Security Applications Conference

Preface	ix
Conference Committee	x
Program Committee	x
Reviewers	xi
Steering Committee	xiii
Sponsors	xiv

Distinguished Practitioner

Privacy and Security in Public Health: Maintaining the Delicate Balance between Personal Privacy and Population Safety	3
<i>Dixie Baker</i>	

Session: Applied Distributed Collaboration

Shamon: A System for Distributed Mandatory Access Control	23
<i>Jonathan McCune, Stefan Berger, Ramón Cáceres, Trent Jaeger, and Reiner Sailer</i>	
A Framework for a Collaborative DDoS Defense	33
<i>George Oikonomou, Jelena Mirkovic, Peter Reiher, and Max Robinson</i>	
V-COPS: A Vulnerability-Based Cooperative Alert Distribution System	43
<i>Shiping Chen, Dongyu Liu, Songqing Chen, and Susbil Jajodia</i>	

Session: Client Access in Untrusted Environments

Delegate: A Proxy Based Architecture for Secure Website Access from an Untrusted Machine	57
<i>Ravi Chandra Jammalamadaka, Timothy W. van der Horst, Sharad Mehrotra, Kent E. Seamons, and Nalini Venkatasubramanian</i>	
KLASSP: Entering Passwords on a Spyware Infected Machine Using a Shared-Secret Proxy	67
<i>Dinei Florêncio and Cormac Herley</i>	
Vulnerability Analysis of MMS User Agents	77
<i>Collin Mulliner and Giovanni Vigna</i>	

Session: Network Intrusion Detection

Backtracking Algorithmic Complexity Attacks against a NIDS	89
<i>Randy Smith, Cristian Estan, and Somesb Jha</i>	
NetSpy: Automatic Generation of Spyware Signatures for NIDS	99
<i>Hao Wang, Somesb Jha, and Vinod Ganapathy</i>	
Detecting Policy Violations through Traffic Analysis	109
<i>Jeffrey Horton and Rei Safavi-Naini</i>	

Session: Network Security

Practical Attack Graph Generation for Network Defense	121
<i>Kyle Ingols, Richard Lippmann, and Keith Pivowarski</i>	
Secure Distributed Cluster Formation in Wireless Sensor Networks.....	131
<i>Kun Sun, Pai Peng, Peng Ning, and Cliff Wang</i>	
Specification-Based Intrusion Detection in WLANs.....	141
<i>Rupinder Gill, Jason Smith, and Andrew Clark</i>	

Session: Security in Systems

From Languages to Systems: Understanding Practical Application Development in Security-typed Languages.....	153
<i>Boniface Hicks, Kiyan Ahmadizadeh, and Patrick McDaniel</i>	
An Internet Voting System Supporting User Privacy	165
<i>Aggelos Karyias, Michael Korman, and David Walluck</i>	
A Study of Access Control Requirements for Healthcare Systems Based on Audit Trails from Access Logs.....	175
<i>Lillian Røstad and Ole Eidsberg</i>	

Invited Essayist

Engineering Sufficiently Secure Computing.....	187
<i>Brian Witten</i>	

Session: Applied Sandboxing

A Module System for Isolating Untrusted Software Extensions.....	203
<i>Philip Fong and Simon Orr</i>	
How to Automatically and Accurately Sandbox Microsoft IIS.....	213
<i>Wei Li, Lap-chung Lam, and Tzi-cker Chiueh</i>	
Data Sandboxing: A Technique for Enforcing Confidentiality Policies.....	223
<i>Tejas Khatiwala, Raj Swaminathan, and V.N. Venkatesh</i>	

Session: Malware

On Detecting Camouflaging Worm	235
<i>Wei Yu, Xun Wang, Prasad Calyam, Dong Xuan, and Wei Zhao</i>	
Bluetooth Worms: Models, Dynamics, and Defense Implications	245
<i>Guanhua Yan and Stephan Eidenbenz</i>	
Back to the Future: A Framework for Automatic Malware Removal and System Repair.....	257
<i>Francis Hsu, Hao Chen, Thomas Ristenpart, Jason Li, and Zhendong Su</i>	

Session: Applied Detection Technologies

Static Detection of Vulnerabilities in x86 Executables	269
<i>Greg Banks, Marco Cova, Viktoria Felmetsger, and Giovanni Vigna</i>	
Foreign Code Detection on the Windows/X86 Platform	279
<i>Susanta Nanda, Wei Li, Lap-Chung Lam, and Tzi-cker Chiueh</i>	
PolyUnpack: Automating the Hidden-Code Extraction of Unpack-Executing Malware	289
<i>Paul Royal, Mitch Halpin, David Dagon, Robert Edmonds, and Wenke Lee</i>	

Classic Papers

Fifteen Years after TX: A Look Back at High Assurance Multi-Level Secure Windowing	301
<i>Jeremy Epstein</i>	
Risks of Untrustworthiness	321
<i>Peter G. Neumann</i>	

Session: Applied Randomization

Address-Space Randomization for Windows Systems	329
<i>Lixin Li, James Just, and R. Sekar</i>	
Address Space Layout Permutation (ASLP): Towards Fine-Grained Randomization of Commodity Software	339
<i>Chongkyung Kil, Jinsuk Jun, Christopher Bookholt, Jun Xu, and Peng Ning</i>	
Known/Chosen Key Attacks against Software Instruction Set Randomization	349
<i>Yoav Weiss and Elena Gabriela Barrantes</i>	

Session: Intrusion Detection

Automatic Evaluation of Intrusion Detection Systems	361
<i>Frédéric Massicotte, François Gagnon, Yvan Labiche, Lionel Briand, and Mathieu Couture</i>	
Offloading IDS Computation to the GPU	371
<i>Nigel Jacob and Carla Brodley</i>	
Anomaly Based Web Phishing Page Detection	381
<i>Ying Pan and Xubua Ding</i>	

Session: Messaging Security

Addressing SMTP-Based Mass-Mailing Activity within Enterprise Networks	393
<i>David Whyte, Paul van Oorschot, and Evangelos Kranakis</i>	
Using Attribute-Based Access Control to Enable Attribute-Based Messaging	403
<i>Rakesh Bobba, Omid Fatemeh, Fariba Khan, Carl Gunter, and Himanshu Khurana</i>	
Enhancing Collaborative Spam Detection with Bloom Filters	414
<i>Jeff Yan and Pook Leong Cho</i>	

Session: Countermeasures

Extended Protection against Stack Smashing Attacks without Performance Loss.....	429
<i>Yves Younan, Davide Pozza, Frank Piessens, and Wouter Joosen</i>	
PAST : Probabilistic Authentication of Sensor Timestamps	439
<i>Asbish Gebani and Surendar Chandra</i>	
Towards Database Firewall: Mining the Damage Spreading Patterns	449
<i>Kun Bai and Peng Liu</i>	

Session: Information Flow and Leakage

A General Dynamic Information Flow Tracking Framework for Security Applications	463
<i>Lap Chung Lam and Tzi-cker Chiueh</i>	
Covert and Side Channels due to Processor Architecture.....	473
<i>Zhengbong Wang and Ruby Lee</i>	
CryptoPage: An Efficient Secure Architecture with Memory Encryption, Integrity and Information Leakage Protection.....	483
<i>Guillaume Duc and Ronan Keryell</i>	
Protecting Privacy in Key-Value Search Systems	493
<i>Yinglian Xie, David O'Hallaron, and Michael Reiter</i>	
Author Index	505