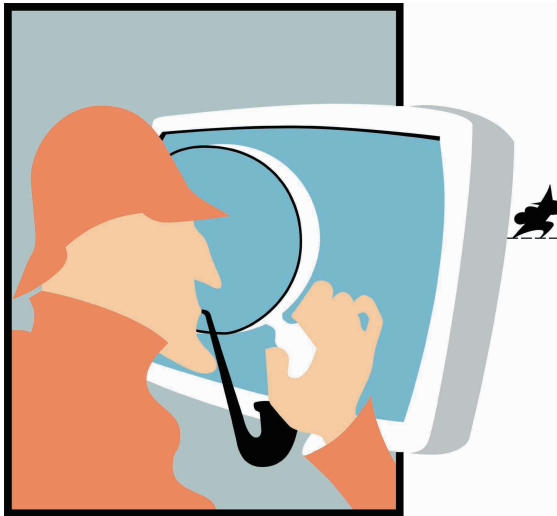


Proceedings

Twenty-Third Annual Computer Security Applications Conference



ACSAC 2007

10-14 December 2007 • Miami Beach, Florida

Sponsored by

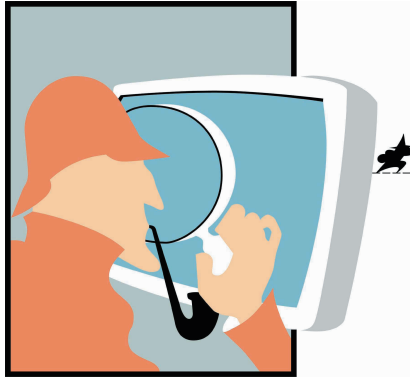
Applied Computer Security Associates



Los Alamitos, California
Washington • Tokyo



Proceedings



ACSAC 2007

Table of Contents

Welcome from the Conference Chair	x
Welcome from the Program Chairs	xi
Conference Committee	xii
Program Committee	xiii
Additional Reviewers and Tutorial Reviewers	xiv
ACSAC Steering Committee	xv
Sponsor: Applied Computer Security Associates	xvi

Distinguished Practitioner

So You Think You Can Dance?	3
<i>Richard A. Kemmerer</i>	

Operating Systems Security and Trusted Computing

Establishing and Sustaining System Integrity via Root of Trust Installation	19
<i>Luke St. Clair, Joshua Schiffman, Trent Jaeger, and Patrick McDaniel</i>	
Tampering with Special Purpose Trusted Computing Devices: A Case Study in Optical Scan E-Voting.....	30
<i>Aggelos Kiayias, Laurent Michel, Alexander Russell, Narasimha Shashidhar, Andrew See, Alexander Shvartsman, and Seda Davtyan</i>	

Toward a Medium-Robustness Separation Kernel Protection Profile40
Rance J. DeLong, Thuy D. Nguyen, Cynthia E. Irvine, and Timothy E. Levin

Malware and Intrusion Detection

Improving Signature Testing through Dynamic Data Flow Analysis.....53
Christopher Kruegel, Davide Balzarotti, William Robertson, and Giovanni Vigna

HoneyIM: Fast Detection and Suppression of Instant Messaging Malware
in Enterprise-Like Networks.....64
Mengjun Xie, Zhenyu Wu, and Haining Wang

Feature Omission Vulnerabilities: Thwarting Signature Generation
for Polymorphic Worms74
Matthew Van Gundy, Hao Chen, Zhendong Su, and Giovanni Vigna

Database Security

Toward Realistic and Artifact-Free Insider-Threat Data87
Kevin S. Killourhy and Roy A. Maxion

Database Isolation and Filtering against Data Corruption Attacks97
Meng Yu, Wanyu Zang, and Peng Liu

Sania: Syntactic and Semantic Analysis for Automated Testing against SQL Injection..... 107
Yuji Kosuga, Kenji Kono, Miyuki Hanaoka, Miho Hishiyama, and Yu Takahama

Applied Cryptography

Closed-Circuit Unobservable Voice over IP..... 119
Carlos Aguilar Melchor, Yves Deswarte, and Julien Iguchi-Cartigny

SSARES: Secure Searchable Automated Remote Email Storage..... 129
Adam J. Aviv, Michael E. Locasto, Shaya Potter, and Angelos D. Keromytis

Misuse Detection and Forensics

The Design and Development of an Undercover Multipurpose Anti-spoofing
Kit (UnMask)..... 141
*Sudhir Aggarwal, Jasbinder Bali, Zhenhai Duan, Leo Kermes,
Wayne Liu, Shahank Sahai, and Zhenghui Zhu*

Efficiency Issues of Rete-Based Expert Systems for Misuse Detection..... 151
Michael Meier, Ulrich Flegel, and Sebastian Schmerl

Tracking Darkports for Network Defense 161
David Whyte, Paul C. van Oorschot, and Evangelos Kranakis

Invited Essayist

Personal Privacy without Computational Obscurity: Rethinking Privacy Protection Strategies for Open Information Networks.....	173
<i>Daniel J. Weitzner</i>	

Classic Paper

Distributed Secure Systems: Then and Now	177
<i>Brian Randell and John Rushby</i>	

Access Control

Extensible Pre-authentication Kerberos.....	201
<i>Phillip L. Hellewell, Timothy W. van der Horst, and Kent E. Seamons</i>	
Quarantining Untrusted Entities: Dynamic Sandboxing Using LEAP	211
<i>Manigandan Radhakrishnan and Jon A. Solworth</i>	
Retrofitting the IBM POWER Hypervisor to Support Mandatory Access Control	221
<i>Enriquillo Valdez, Reiner Sailer, and Ronald Perez</i>	

Wireless and Mobile Systems Security

Extending the Java Virtual Machine to Enforce Fine-Grained Security Policies in Mobile Devices.....	233
<i>Iulia Ion, Boris Dragovic, and Bruno Crispo</i>	
Countering False Accusations and Collusion in the Detection of In-Band Wormholes	243
<i>Daniel Sterne, Geoffrey Lawler, Richard Gopaul, Brian Rivera, Kelvin Marcus, and Peter Kruus</i>	
Efficient Distributed Detection of Node Replication Attacks in Sensor Networks	257
<i>Bo Zhu, Venkata Gopala Krishna Addada, Sanjeev Setia, Sushil Jajodia, and Sankardas Roy</i>	

Security Engineering

Security Usability Principles for Vulnerability Analysis and Risk Assessment	269
<i>Audun Jøsang, Bander AlFayyadh, Tyrone Grandison, Mohammed AlZomai, and Judith McNamara</i>	
Breaking Visual CAPTCHAs with Naïve Pattern Recognition Algorithms	279
<i>Jeff Yan and Ahmad Salah El Ahmad</i>	

Combining Static and Dynamic Analysis for Automatic Identification of Precise Access-Control Policies	292
<i>Paolina Centonze, Robert J. Flynn, and Marco Pistoia</i>	

Security in P2P Systems

Routing in the Dark: Pitch Black.....	305
<i>Nathan S. Evans, Chris GauthierDickey, and Christian Grothoff</i>	
Centralized Security Labels in Decentralized P2P Networks.....	315
<i>Nathalie Tsybulnik, Kevin W. Hamlen, and Bhavani Thuraisingham</i>	
A Taxonomy of Botnet Structures	325
<i>David Dagon, Guofei Gu, Christopher P. Lee, and Wenke Lee</i>	

Distributed Systems Security

An Overview of the Annex System	341
<i>D. A. Grove, T. C. Murray, C. A. Owen, C. J. North, J. A. Jones, M. R. Beaumont, and B. D. Hopkins</i>	
Efficient Detection of Delay-Constrained Relay Nodes	353
<i>Baris Coskun and Nasir Memon</i>	
Bonsai: Balanced Lineage Authentication.....	363
<i>Ashish Gehani and Ulf Lindqvist</i>	

Software and Applications Security

Secure Input for Web Applications	375
<i>Martin Szydlowski, Christopher Kruegel, and Engin Kirda</i>	
Secure and Flexible Monitoring of Virtual Machines	385
<i>Bryan D. Payne, Martim D. P. de A. Carbone, and Wenke Lee</i>	
Automated Format String Attack Prevention for Win32/X86 Binaries.....	398
<i>Wei Li and Tzi-cker Chiueh</i>	

Malware

MetaAware: Identifying Metamorphic Malware	411
<i>Qinghua Zhang and Douglas S. Reeves</i>	
Limits of Static Analysis for Malware Detection	421
<i>Andreas Moser, Christopher Kruegel, and Engin Kirda</i>	
OmniUnpack: Fast, Generic, and Safe Unpacking of Malware.....	431
<i>Lorenzo Martignoni, Mihai Christodorescu, and Somesh Jha</i>	

Assurance

Channels: Runtime System Infrastructure for Security-Typed Languages.....	443
<i>Boniface Hicks, Tim Misiak, and Patrick McDaniel</i>	
Automated Security Debugging Using Program Structural Constraints.....	453
<i>Chongkyung Kil, Emre Can Sezer, Peng Ning, and Xiaolan Zhang</i>	
Fine-Grained Information Flow Analysis and Enforcement in a Java Virtual Machine.....	463
<i>Deepak Chandra and Michael Franz</i>	

Software Security

Automated Vulnerability Analysis: Leveraging Control Flow for Evolutionary Input Crafting	477
<i>Sherri Sparks, Shawn Embleton, Ryan Cunningham, and Cliff Zou</i>	
The Age of Data: Pinpointing Guilty Bytes in Polymorphic Buffer Overflows on Heap or Stack.....	487
<i>Asia Slowinska and Herbert Bos</i>	
Spector: Automatically Analyzing Shell Code	501
<i>Kevin Borders, Atul Prakash, and Mark Zielinski</i>	

Author Index	515
---------------------------	-----