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
Richard A. Kemmerer

Operating Systems Security and Trusted Computing

Establishing and Sustaining System Integrity via Root of Trust Installation ...........................................19
Luke St. Clair, Joshua Schiffman, Trent Jaeger, and Patrick McDaniel

Tampering with Special Purpose Trusted Computing Devices: A Case Study in Optical Scan E-Voting ..........................................................30
Aggelos Kiayias, Laurent Michel, Alexander Russell, Narasimha Shashidhar, Andrew See, Alexander Shvartsman, and Seda Davtyan
Toward a Medium-Robustness Separation Kernel Protection Profile ................................................................. 40
  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 Worms .......................................................... 74
  Matthew Van Gundy, Hao Chen, Zhendong Su, and Giovanni Vigna

Database Security

Toward Realistic and Artifact-Free Insider-Threat Data ............................................................................. 87
  Kevin S. Killourhy and Roy A. Maxion

Database Isolation and Filtering against Data Corruption Attacks .......................................................... 97
  Meng Yu, Wanyu Zang, and Feng 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

Daniel J. Weitzner

Classic Paper

Distributed Secure Systems: Then and Now

Brian Randell and John Rushby

Access Control

Extensible Pre-authentication Kerberos

Phillip L. Hellewell, Timothy W. van der Horst, and Kent E. Seamons

Quarantining Untrusted Entities: Dynamic Sandboxing Using LEAP

Manigandan Radhakrishnan and Jon A. Solworth

Retrofitting the IBM POWER Hypervisor to Support Mandatory Access Control

Enriquillo Valdez, Reiner Sailer, and Ronald Perez

Wireless and Mobile Systems Security

Extending the Java Virtual Machine to Enforce Fine-Grained Security Policies in Mobile Devices

Iulia Ion, Boris Dragovic, and Bruno Crispo

Countering False Accusations and Collusion in the Detection of In-Band Wormholes

Daniel Sterne, Geoffrey Lawler, Richard Gopaul, Brian Rivera, Kelvin Marcus, and Peter Kruus

Efficient Distributed Detection of Node Replication Attacks in Sensor Networks

Bo Zhu, Venkata Gopala Krishna Addada, Sanjeev Setia, Sushil Jajodia, and Sankardas Roy

Security Engineering

Security Usability Principles for Vulnerability Analysis and Risk Assessment

Audun Jøsang, Bander AlFayyadh, Tyrone Grandison, Mohammed AlZomai, and Judith McNamara

Breaking Visual CAPTCHAs with Naïve Pattern Recognition Algorithms

Jeff Yan and Ahmad Salah El Ahmad
Combining Static and Dynamic Analysis for Automatic Identification of Precise Access-Control Policies
Paolina Centonze, Robert J. Flynn, and Marco Pistoia

Security in P2P Systems
Routing in the Dark: Pitch Black
Nathan S. Evans, Chris Gauthier-Dickey, and Christian Grothoff
Centralized Security Labels in Decentralized P2P Networks
Nathalie Tsybulnik, Kevin W. Hamlen, and Bhavani Thuraisingham
A Taxonomy of Botnet Structures
David Dagon, Guofei Gu, Christopher P. Lee, and Wenke Lee

Distributed Systems Security
An Overview of the Annex System
Efficient Detection of Delay-Constrained Relay Nodes
Baris Coskun and Nasir Memon
Bonsai: Balanced Lineage Authentication
Ashish Gehani and Ulf Lindqvist

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

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

Channels: Runtime System Infrastructure for Security-Typed Languages.................................................................443
  Boniface Hicks, Tim Misiak, and Patrick McDaniel

Automated Security Debugging Using Program Structural Constraints.................................................................453
  Chongkyung Kil, Emre Can Sezer, Peng Ning, and Xiaolan Zhang

Fine-Grained Information Flow Analysis and Enforcement in a Java Virtual Machine..................................................463
  Deepak Chandra and Michael Franz

Software Security

Automated Vulnerability Analysis: Leveraging Control Flow for Evolutionary Input Crafting .................................................................477
  Sherri Sparks, Shawn Embleton, Ryan Cunningham, and Cliff Zou

The Age of Data: Pinpointing Guilty Bytes in Polymorphic Buffer Overflows on Heap or Stack.................................................................487
  Asia Slowinska and Herbert Bos

Spector: Automatically Analyzing Shell Code..................................................................................................................501
  Kevin Borders, Atul Prakash, and Mark Zielinski

Author Index ..................................................................................................................................................515