# Table of Contents

Message from the General Chair ................................................................. ix  
Message from the Program Chairs ........................................................... ix  
Conference Committee .............................................................................. xi  
Program Committee .................................................................................. xii  
Additional Reviewers .............................................................................. xiii  
Tutorial Reviewers ................................................................................... xiv  
Sponsor ....................................................................................................... xv  
ACSAC Committee .................................................................................... xvi

## Discovering Policy

A Network Access Control Mechanism Based on Behavior Profiles ................................................................. 3  
*Vanessa Frias-Martinez, Joseph Sherrick, Salvatore J. Stolfo, and Angelos D. Keromytis*

RoleVAT: Visual Assessment of Practical Need for Role Based Access Control ..................................................... 13  
*Dana Zhang, Kotagiri Ramamohanarao, Steven Versteeg, and Rui Zhang*

How to Securely Break into RBAC: The BTG-RBAC Model .................................................................................. 23  
*Ana Ferreira, David Chadwick, Pedro Farinha, Ricardo Correia, Gansen Zao, Rui Chilro, and Luis Antunes*

## Invited Paper

Computer-Related Risk Futures ................................................................. 35  
*Peter G. Neumann*

## Hardware/Software Security

Evaluation of a DPA-Resistant Prototype Chip .................................................................................................. 43  
*Mario Kirschbaum and Thomas Popp*

FPValidator: Validating Type Equivalence of Function Pointers on the Fly ......................................................... 51  
*Hua Wang, Yao Guo, and Xiangqun Chen*

Surgically returning to randomized lib(c) ............................................................................................................. 60  
*Giampaolo Fresi Roglia, Lorenzo Martignoni, Roberto Paleari, and Danilo Bruschi*
Cloud Security

SecureMR: A Service Integrity Assurance Framework for MapReduce
Wei Wei, Juan Du, Ting Yu, and Xiaohui Gu

Justifying Integrity Using a Virtual Machine Verifier
Joshua Schiffman, Thomas Moyer, Christopher Shal, Trent Jaeger, and Patrick McDaniel

Integrity

Scalable Web Content Attestation
Thomas Moyer, Kevin Butler, Joshua Schiffman, Patrick McDaniel, and Trent Jaeger

A Study of User-Friendly Hash Comparison Schemes
Hsu-Chun Hsiao, Yue-Hsun Lin, Ahren Studer, Cassandra Studer, King-Hang Wang, Hiroaki Kikuchi, Adrian Perrig, Hung-Min Sun, and Bo-Yin Yang

Network Security

Modeling Modern Network Attacks and Countermeasures Using Attack Graphs
Kyle Ingols, Matthew Chu, Richard Lippmann, Seth Webster, and Stephen Boyer

Evaluating Network Security with Two-Layer Attack Graphs
Anming Xie, Zhuhua Cai, Cong Tang, Jianbin Hu, and Zhong Chen

Intellectual Property Rights

Unifying Broadcast Encryption and Traitor Tracing for Content Protection
Hongxia Jin and Jeffrey Lotspiech

Detecting Software Theft via System Call Based Birthmarks
Xinran Wang, Yoon-Chan Jhi, Sencun Zhu, and Peng Liu

Classic Paper I

Reflections on UNIX Vulnerabilities
Matt Bishop

Invited Essayist

The Good, the Bad, and the Ugly: Stepping on the Security Scale
Mary Ann Davidson

Authentication and Audit

A New Approach for Anonymous Password Authentication
Yanjiang Yang, Jianying Zhou, Jian Weng, and Feng Bao

On the Security of PAS (Predicate-Based Authentication Service)
Shujun Li, Hassan Jameel Asghar, Josef Pieprzyk, Ahmad-Reza Sadeghi, Roland Schmitz, and Huaxiong Wang
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>BAF: An Efficient Publicly Verifiable Secure Audit Logging Scheme for Distributed Systems</td>
<td>219</td>
</tr>
<tr>
<td>Attila Altay Yavuz and Peng Ning</td>
<td></td>
</tr>
<tr>
<td>Malware, Botnets andOperating System Security (Part 1)</td>
<td></td>
</tr>
<tr>
<td>FIRE: Finding Rogue nEtworks</td>
<td>231</td>
</tr>
<tr>
<td>Brett Stone-Gross, Christopher Kruegel, Kevin Almeroth, Andreas Moser, and Engin Kirda</td>
<td></td>
</tr>
<tr>
<td>Active Botnet Probing to Identify Obscure Command and Control Channels</td>
<td>241</td>
</tr>
<tr>
<td>Guofei Gu, Vinod Yegneswaran, Phillip Porras, Jennifer Stoll, and Wenke Lee</td>
<td></td>
</tr>
<tr>
<td>TrustGraph: Trusted Graphics Subsystem for High Assurance Systems</td>
<td>254</td>
</tr>
<tr>
<td>Hamed Okhravi and David M. Nicol</td>
<td></td>
</tr>
<tr>
<td>Denial of Service Defense</td>
<td></td>
</tr>
<tr>
<td>RAD: Reflector Attack Defense Using Message Authentication Codes</td>
<td>269</td>
</tr>
<tr>
<td>Erik Kline, Matt Beaumont-Gay, Jelena Mirkovic, and Peter Reiher</td>
<td></td>
</tr>
<tr>
<td>A Guided Tour Puzzle for Denial of Service Prevention</td>
<td>279</td>
</tr>
<tr>
<td>Mehmud Abliz and Taieb Znati</td>
<td></td>
</tr>
<tr>
<td>Online Signature Generation for Windows Systems</td>
<td>289</td>
</tr>
<tr>
<td>Lixin Li, James E. Just, and R. Sekar</td>
<td></td>
</tr>
<tr>
<td>Malware, Botnets and Operating System Security (Part 2)</td>
<td></td>
</tr>
<tr>
<td>Protecting Commodity Operating System Kernels from Vulnerable Device Drivers</td>
<td>301</td>
</tr>
<tr>
<td>Shakeel Butt, Vinod Ganapathy, Michael M. Swift, and Chih-Cheng Chang</td>
<td></td>
</tr>
<tr>
<td>Detecting Malicious Flux Service Networks through Passive Analysis of Recursive DNS Traces</td>
<td>311</td>
</tr>
<tr>
<td>Roberto Perdisci, Igino Corona, David Dagon, and Wenke Lee</td>
<td></td>
</tr>
<tr>
<td>Identification of Bot Commands by Run-Time Execution Monitoring</td>
<td>321</td>
</tr>
<tr>
<td>Younghoe Park and Douglas S. Reeves</td>
<td></td>
</tr>
<tr>
<td>Mobile Security</td>
<td></td>
</tr>
<tr>
<td>Transparent Encryption for External Storage Media with Key Management Adapted to Mobile Use</td>
<td>333</td>
</tr>
<tr>
<td>Alf Zugenmaier, Sven Lachmund, and Dileesh Jostin</td>
<td></td>
</tr>
<tr>
<td>Machigar Ongtang, Stephen McLaughlin, William Enck, and Patrick McDaniel</td>
<td></td>
</tr>
<tr>
<td>Leveraging Cellular Infrastructure to Improve Fraud Prevention</td>
<td>350</td>
</tr>
<tr>
<td>Frank S. Park, Chinmay Gangakhedkar, and Patrick Traynor</td>
<td></td>
</tr>
<tr>
<td>Multimedia and Web Security</td>
<td></td>
</tr>
<tr>
<td>Analyzing and Detecting Malicious Flash Advertisements</td>
<td>363</td>
</tr>
<tr>
<td>Sean Ford, Marco Cova, Christopher Kruegel, and Giovanni Vigna</td>
<td></td>
</tr>
<tr>
<td>Symmetric Cryptography in Javascript</td>
<td>373</td>
</tr>
<tr>
<td>Emily Stark, Michael Hamburg, and Dan Boneh</td>
<td></td>
</tr>
</tbody>
</table>
Analyzing Information Flow in JavaScript-Based Browser Extensions

Mohan Dhawan and Vinod Ganapathy

Classic Paper II

Java Security: A Ten Year Retrospective

Li Gong

Trust Management

Secure Web 2.0 Content Sharing Beyond Walled Gardens

San-Tsai Sun, Kirstie Hawkey, and Konstantin Beznosov

Enabling Secure Secret Sharing in Distributed Online Social Networks

Le-Hung Vu, Karl Aberer, Sonja Buchegger, and Anwitaman Datta

Deploying and Monitoring DNS Security (DNSSEC)

Eric Osterweil, Dan Massey, and Lixia Zhang

Virtualization Security

MAVMM: Lightweight and Purpose Built VMM for Malware Analysis

Anh M. Nguyen, Nabil Schear, HeeDong Jung, Apeksha Godiyal, Samuel T. King, and Hai D. Nguyen

Protecting Kernel Code and Data with a Virtualization-Aware Collaborative Operating System

Daniela Alvim Seabra de Oliveira and S. Felix Wu

HIMA: A Hypervisor-Based Integrity Measurement Agent

Ahmed M. Azab, Peng Ning, Emre C. Sezer, and Xiaolan Zhang

Intrusion Detection, Recovery and Analysis

Online Sketching of Network Flows for Real-Time Stepping-Stone Detection

Baris Coskun and Nasir Memon

SHELF: Preserving Business Continuity and Availability in an Intrusion Recovery System

Xi Xiong, Xiaoqi Jia, and Peng Liu

An Empirical Approach to Modeling Uncertainty in Intrusion Analysis

Xinming Ou, Siva Raj Rajagopalan, and Sakthiyarajak Sakthivelmurugan

Privacy and Software Assurance

The Design of a Trustworthy Voting System

Nathanael Paul and Andrew S. Tanenbaum

Privacy through Noise: A Design Space for Private Identification

Karsten Nohl and David Evans

A Survey of Vendor Software Assurance Practices

Jeremy Epstein

Author Index