

2009 Annual Computer Security Applications Conference

(ACSAC 2009)

**Honolulu, Hawaii, USA
7-11 December 2009**



IEEE Catalog Number: CFP09393-PRT
ISBN: 978-1-4244-5327-6

Table of Contents



Message from the General Chair	
Message from the Program Chairs	
Conference Committee	
Program Committee	
Additional Reviewers	
Tutorial Reviewers	
Sponsor	
ACSAC Committee	

Discovering Policy

A Network Access Control Mechanism Based on Behavior Profiles	3
<i>Vanessa Frias-Martinez, Joseph Sherrick, Salvatore J. Stolfo, and Angelos D. Keromytis</i>	
RoleVAT: Visual Assessment of Practical Need for Role Based Access Control	13
<i>Dana Zhang, Kotagiri Ramamohanarao, Steven Versteeg, and Rui Zhang</i>	
How to Securely Break into RBAC: The BTG-RBAC Model	23
<i>Ana Ferreira, David Chadwick, Pedro Farinha, Ricardo Correia, Gansen Zao, Rui Chilro, and Luis Antunes</i>	

Invited Paper

Computer-Related Risk Futures	35
<i>Peter G. Neumann</i>	

Hardware/Software Security

Evaluation of a DPA-Resistant Prototype Chip	43
<i>Mario Kirschbaum and Thomas Popp</i>	
FPValidator: Validating Type Equivalence of Function Pointers on the Fly	51
<i>Hua Wang, Yao Guo, and Xiangqun Chen</i>	
Surgically returning to randomized lib(c).....	60
<i>Giampaolo Fresi Roglia, Lorenzo Martignoni, Roberto Paleari, and Danilo Bruschi</i>	

Cloud Security

SecureMR: A Service Integrity Assurance Framework for MapReduce 73
Wei Wei, Juan Du, Ting Yu, and Xiaohui Gu

Justifying Integrity Using a Virtual Machine Verifier 83
Joshua Schiffman, Thomas Moyer, Christopher Shal, Trent Jaeger, and Patrick McDaniel

Integrity

Scalable Web Content Attestation 95
Thomas Moyer, Kevin Butler, Joshua Schiffman, Patrick McDaniel, and Trent Jaeger

A Study of User-Friendly Hash Comparison Schemes 105
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 117
Kyle Ingols, Matthew Chu, Richard Lippmann, Seth Webster, and Stephen Boyer

Evaluating Network Security with Two-Layer Attack Graphs 127
Anming Xie, Zhuhua Cai, Cong Tang, Jianbin Hu, and Zhong Chen

Intellectual Property Rights

Unifying Broadcast Encryption and Traitor Tracing for Content Protection 139
Hongxia Jin and Jeffrey Lotspiech

Detecting Software Theft via System Call Based Birthmarks 149
Xinran Wang, Yoon-Chan Jhi, Sencun Zhu, and Peng Liu

Classic Paper I

Reflections on UNIX Vulnerabilities 161
Matt Bishop

Invited Essayist

The Good, the Bad, and the Ugly: Stepping on the Security Scale 187
Mary Ann Davidson

Authentication and Audit

A New Approach for Anonymous Password Authentication 199
Yanjiang Yang, Jianying Zhou, Jian Weng, and Feng Bao

On the Security of PAS (Predicate-Based Authentication Service) 209
Shujun Li, Hassan Jameel Asghar, Josef Pieprzyk, Ahmad-Reza Sadeghi, Roland Schmitz, and Huaxiong Wang

BAF: An Efficient Publicly Verifiable Secure Audit Logging Scheme for Distributed Systems.....	219
<i>Attila Altay Yavuz and Peng Ning</i>	

Malware, Botnets and Operating System Security (Part 1)

FIRE: FInding Rogue nEtworks	231
<i>Brett Stone-Gross, Christopher Kruegel, Kevin Almeroth, Andreas Moser, and Engin Kirda</i>	
Active Botnet Probing to Identify Obscure Command and Control Channels	241
<i>Guofei Gu, Vinod Yegneswaran, Phillip Porras, Jennifer Stoll, and Wenke Lee</i>	
TrustGraph: Trusted Graphics Subsystem for High Assurance Systems.....	254
<i>Hamed Okhravi and David M. Nicol</i>	

Denial of Service Defense

RAD: Reflector Attack Defense Using Message Authentication Codes	269
<i>Erik Kline, Matt Beaumont-Gay, Jelena Mirkovic, and Peter Reiher</i>	
A Guided Tour Puzzle for Denial of Service Prevention.....	279
<i>Mehmud Abliz and Taieb Znati</i>	
Online Signature Generation for Windows Systems	289
<i>Lixin Li, James E. Just, and R. Sekar</i>	

Malware, Botnets and Operating System Security (Part 2)

Protecting Commodity Operating System Kernels from Vulnerable Device Drivers	301
<i>Shakeel Butt, Vinod Ganapathy, Michael M. Swift, and Chih-Cheng Chang</i>	
Detecting Malicious Flux Service Networks through Passive Analysis of Recursive DNS Traces	311
<i>Roberto Perdisci, Iginio Corona, David Dagon, and Wenke Lee</i>	
Identification of Bot Commands by Run-Time Execution Monitoring	321
<i>Younghee Park and Douglas S. Reeves</i>	

Mobile Security

Transparent Encryption for External Storage Media with Key Management Adapted to Mobile Use.....	333
<i>Alf Zugenmaier, Sven Lachmund, and Dileesh Jostin</i>	
Semantically Rich Application-Centric Security in Android	340
<i>Machigar Ongtang, Stephen McLaughlin, William Enck, and Patrick McDaniel</i>	
Leveraging Cellular Infrastructure to Improve Fraud Prevention.....	350
<i>Frank S. Park, Chinmay Gangakhedkar, and Patrick Traynor</i>	

Multimedia and Web Security

Analyzing and Detecting Malicious Flash Advertisements	363
<i>Sean Ford, Marco Cova, Christopher Kruegel, and Giovanni Vigna</i>	
Symmetric Cryptography in Javascript.....	373
<i>Emily Stark, Michael Hamburg, and Dan Boneh</i>	

Analyzing Information Flow in JavaScript-Based Browser Extensions	382
<i>Mohan Dhawan and Vinod Ganapathy</i>	

Classic Paper II

Java Security: A Ten Year Retrospective	395
<i>Li Gong</i>	

Trust Management

Secure Web 2.0 Content Sharing Beyond Walled Gardens	409
<i>San-Tsai Sun, Kirstie Hawkey, and Konstantin Beznosov</i>	

Enabling Secure Secret Sharing in Distributed Online Social Networks	419
<i>Le-Hung Vu, Karl Aberer, Sonja Buchegger, and Anwitaman Datta</i>	

Deploying and Monitoring DNS Security (DNSSEC)	429
<i>Eric Osterweil, Dan Massey, and Lixia Zhang</i>	

Virtualization Security

MAVMM: Lightweight and Purpose Built VMM for Malware Analysis	441
<i>Anh M. Nguyen, Nabil Schear, HeeDong Jung, Apeksha Godiyal, Samuel T. King, and Hai D. Nguyen</i>	

Protecting Kernel Code and Data with a Virtualization-Aware Collaborative Operating System	451
<i>Daniela Alvim Seabra de Oliveira and S. Felix Wu</i>	

HIMA: A Hypervisor-Based Integrity Measurement Agent	461
<i>Ahmed M. Azab, Peng Ning, Emre C. Sezer, and Xiaolan Zhang</i>	

Intrusion Detection, Recovery and Analysis

Online Sketching of Network Flows for Real-Time Stepping-Stone Detection	473
<i>Baris Coskun and Nasir Memon</i>	

SHELF: Preserving Business Continuity and Availability in an Intrusion Recovery System	484
<i>Xi Xiong, Xiaoqi Jia, and Peng Liu</i>	

An Empirical Approach to Modeling Uncertainty in Intrusion Analysis	494
<i>Xinming Ou, Siva Raj Rajagopalan, and Sakthiyumaraja Sakthivelmurugan</i>	

Privacy and Software Assurance

The Design of a Trustworthy Voting System	507
<i>Nathanael Paul and Andrew S. Tanenbaum</i>	

Privacy through Noise: A Design Space for Private Identification	518
<i>Karsten Nohl and David Evans</i>	

A Survey of Vendor Software Assurance Practices	528
<i>Jeremy Epstein</i>	

Author Index