

Proceedings

Cybersecurity Applications and Technology Conference for Homeland Security

*Washington, D.C.
March 3-4, 2009*



Los Alamitos, California
Washington • Tokyo



TABLE OF CONTENTS

INFORMATION INFRASTRUCTURE SECURITY- DOMAIN NAME SYSTEM SECURITY (DNSSEC)

DNSSEC in Practice: Using DNSSEC-Tools to Deploy DNSSEC..... 1
Suresh Krishnaswamy, Wes Hardaker, Russ Mundy

Information Leakage through the Domain Name System 14
Scott Rose, Ramaswamy Chandramouli, Anastase Nakassis

INFORMATION INFRASTRUCTURE SECURITY- SECURE PROTOCOLS FOR THE ROUTING INFRASTRUCTURE (SPRI)

A Comparative Analysis of BGP Anomaly Detection and Robustness Algorithms20
Kotikapaludi Sriram, Oliver Borchert, Okhee Kim, Patrick Gleichmann, Doug Montgomery

Progress Toward Securing the Routing Infrastructure34
Sandra Murphy, Samuel Weiler

A High Performance Software Architecture for a Secure Internet Routing PKI44
Mark C. Reynolds, Stephen Kent

RESEARCH TOOLS AND TECHNIQUES- CYBER DEFENSE TECHNOLOGY EXPERIMENTAL RESEARCH (DETER)

Current Developments in DETER Cybersecurity Testbed Technology49
Terry Benzel, Bob Braden, Ted Faber, Jelena Mirkovic, Steve Schwab, Karen Sollins, John Wroclawski

RESEARCH TOOLS AND TECHNIQUES- PROTECTED REPOSITORY FOR THE DEFENSE OF INFRASTRUCTURE AGAINST CYBER THREATS (PREDICT)

Uses and Challenges for Network Datasets.....63
John Heidemann, Christos Papadopoulos

Trusted Distributed Repository of Internet Usage Data for Use in Cyber Security Research.....73
Charlotte Scheper, Susanna Cantor, Renee Karlsen

BROAD AGENCY ANNOUNCEMENT 04-17

SYSTEM SECURITY ENGINEERING

Information-Flow Aware Virtual Machines: Foundations for Trustworthy Computing.....79
Michael Franz

Static Analysis of Software Executables.....85
David Melski, Tim Teitelbaum, Thomas Reps

How to Test DoS Defenses	91
<i>Jelena Mirkovic, Sonia Fahmy, Peter Reiher, Roshan K. Thomas</i>	

SECURITY OF OPERATIONAL SYSTEMS

SECURITY AND TRUSTWORTHINESS FOR CRITICAL INFRASTRUCTURE PROTECTION

Virtual Private Groups for Protecting Critical Infrastructure Networks	106
<i>Richard C. O'Brien, Charles N. Payne Jr.</i>	
Advances in Topological Vulnerability Analysis	112
<i>Steven Noel, Matthew Elder, Sushil Jajodia, Pramod Kalapa, Scott O'Hare, Kenneth Prole</i>	
Incrementally-Deployable Security for Interdomain Routing	118
<i>Jennifer Rexford, Joan Feigenbaum</i>	
Towards Fool-Proof Configuration Assessments	123
<i>Rajesh Talpade</i>	

INVESTIGATIVE AND PREVENTION TECHNOLOGIES

NETWORK ATTACK FORENSICS (E.G., TRACEBACK)

Effective Flow Filtering for Botnet Search Space Reduction	129
<i>Robert Walsh, David Lapsley, W. Timothy Strayer</i>	

TECHNOLOGIES TO DEFEND AGAINST IDENTITY THEFT

The PhishBouncer Experience	138
<i>Partha Pal, Michael Atighetchi</i>	
Phisherman: A Phishing Data Repository	143
<i>Gregg Tally</i>	

BROAD AGENCY ANNOUNCEMENT 07-09

BOTNETS AND OTHER MALWARE: DETECTION AND MITIGATION

Global Internet Monitoring Using Passive DNS	149
<i>David Dagon, Wenke Lee</i>	

COMPOSABLE AND SCALABLE SECURE SYSTEMS

Deploying DNS Security (DNSSEC) in Large-Scale Operational Environments	155
<i>Joe Gersch, Dan Massey</i>	
Inter-Network Operations Center Dial-by-ASN (INOC-DBA), a Resource for the Network Operator Community	167
<i>Ross Stapleton-Gray</i>	

NETWORK DATA VISUALIZATION FOR INFORMATION ASSURANCE

- FloVis: Flow Visualization System** 172
Teryl Taylor, Diana Paterson, Joel Glanfield, Carrie Gates, Stephen Brooks, John McHugh
- Visual Analytics for Network Flow Analysis** 185
John R. Goodall, Daniel R. Tesone

INTERNET TOMOGRAPHY / TOPOGRAPHY

- Internet Mapping: From Art to Science**..... 191
Kimberly Claffy, Young Hyun, Ken Keys, Marina Fomenkov, Dmitri Krioukov

ROUTING SECURITY MANAGEMENT TOOL

- BGPmon: A Real-Time, Scalable, Extensible Monitoring System**..... 198
He Yan, Ricardo Oliveira, Kevin Burnett, Dave Matthews, Lixia Zhang, Dan Massey
- BGP Routing Integrity Checker and Prefix-List Filter Generation Tool** 210
Ross Stapleton-Gray

PROCESS CONTROL SYSTEM SECURITY

REAL-TIME SECURITY EVENT ASSESSMENT AND MITIGATION

- Quickdraw: Generating Security Log Events for Legacy SCADA and Control System Devices**..... 213
Dale Peterson

DATA ANONYMIZATION TOOLS AND TECHNIQUES

- The Challenges of Effectively Anonymizing Network Data** 216
Scott E. Coull, Fabian Monrose, Michael K. Reiter, Michael Bailey

INSIDER THREAT DETECTION AND MITIGATION

- Insider Threat Detection Using Graph-Based Approaches**..... 223
William Eberle, Lawrence Holder

SMALL BUSINESS INNOVATION RESEARCH (SBIR)

SBIR 4.1-008: ADVANCED SECURE SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) AND RELATED DISTRIBUTED CONTROL SYSTEMS

- A Secure IEC-61850 Toolkit for Utility Automation** 228
Stanley A. Klein

SBIR 4.2-001: CROSS-DOMAIN ATTACK CORRELATION TECHNOLOGIES

Correlation and Collaboration in Anomaly Detection	234
<i>Richard E. Cullingford</i>	

SBIR 5.2-004: HARDWARE-ASSISTED SYSTEM SECURITY MONITOR

Pattern Recognition without Tradeoffs: Scalable Accuracy with No Impact on Speed.....	238
<i>Rick Dove</i>	

SBIR 6.1-007: NETWORK-BASED BOUNDARY CONTROL

Logical Network Boundary Controller	244
<i>John Wu, Yongdae Kim, Ryan Marotz, Ranga Ramanujan, James Tyra</i>	
Information Assurance Using a Defense In-Depth Strategy.....	250
<i>Kevin Dauch, Adam Hovak, Roger Nestler</i>	

SBIR 6.1-008: BOTNET DETECTION AND MITIGATION

A Combined Fusion and Data Mining Framework for the Detection of Botnets	256
<i>Aggelos Kiayias, Justin Neumann, David Walluck, Owen McCusker</i>	
Real-Time Detection of Fast Flux Service Networks.....	268
<i>Alper Caglayan, Mike Toothaker, Dan Drapeau, Dustin Burke, Gerry Eaton</i>	
Network Malware Capture	276
<i>Christopher Jordan, Alice Chang, Kun Luo</i>	

RAPID TECHNOLOGY APPLICATION PROGRAM (RTAP)

RTAP CS1: BOTNET DETECTION AND MITIGATION

A Survey of Botnet Technology and Defenses	280
<i>Michael Bailey, Evan Cooke, Farnam Jahanian, Yunjing Xu, Manish Karir</i>	

RTAP CS2: EXERCISE SCENARIO MODELING TOOL (ESMT)

The Cyber Scenario Modeling and Reporting Tool (CyberSMART).....	286
<i>Jim Marshall</i>	

EXTENDED ABSTRACTS FOR OTHER FUNDED RESEARCH

SLINGbot: A System for Live Investigation of Next Generation Botnets.....	291
<i>Alden W. Jackson, David Lapsley, Christine Jones, Mudge Zatko, Chaos Golubitsky, W. Timothy Strayer</i>	
Prototyping a Computer-Based Simulation of the Finance Sector	297
<i>Ernest W. Drew III</i>	

Cybersecurity Technology Transition: A Practical Approach.....303
Salvatore C. Paladino, Jason E. Fingerman

Author Index