

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Richard Lippmann Engin Kirda
Ari Trachtenberg (Eds.)

Recent Advances in Intrusion Detection

11th International Symposium, RAID 2008
Cambridge, MA, USA, September 15-17, 2008
Proceedings

Volume Editors

Richard Lippmann
Lincoln Laboratory
Massachusetts Institute of Technology
Lexington, MA, USA
E-mail: lippmann@ll.mit.edu

Engin Kirda
Institut Eurecom
Sophia-Antipolis, France
E-mail: engin.kirda@eurecom.fr

Ari Trachtenberg
Boston University
Boston, MA, USA
E-mail: trachten@bu.edu

Library of Congress Control Number: 2008934305

CR Subject Classification (1998): K.6.5, K.4, E.3, C.2, D.4.6

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-87402-X Springer Berlin Heidelberg New York
ISBN-13 978-3-540-87402-7 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2008
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12511846 06/3180 5 4 3 2 1 0

Preface

On behalf of the Program Committee, it is our pleasure to present the proceedings of the 11th International Symposium on Recent Advances in Intrusion Detection (RAID 2008), which took place in Cambridge, Massachusetts, USA on September 15–17.

The symposium brought together leading researchers and practitioners from academia, government and industry to discuss intrusion detection research and practice. There were six main sessions presenting full-fledged research papers (rootkit prevention, malware detection and prevention, high performance intrusion and evasion, web application testing and evasion, alert correlation and worm detection, and anomaly detection and network traffic analysis), a session of posters on emerging research areas and case studies, and two panel discussions (“Government Investments: Successes, Failures and the Future” and “Life after Antivirus - What Does the Future Hold?”).

The RAID 2008 Program Committee received 80 paper submissions from all over the world. All submissions were carefully reviewed by at least three independent reviewers on the basis of space, topic, technical assessment, and overall balance. Final selection took place at the Program Committee meeting on May 23rd in Cambridge, MA. Twenty papers were selected for presentation and publication in the conference proceedings, and four papers were recommended for resubmission as poster presentations.

As a new feature this year, the symposium accepted submissions for poster presentations, which have been published as extended abstracts, reporting early-stage research, demonstration of applications, or case studies. Thirty-nine posters were submitted for a numerical review by an independent, three-person subcommittee of the Program Committee based on novelty, description, and evaluation. The subcommittee chose to recommend the acceptance of 16 of these posters for presentation and publication.

The success of RAID 2008 depended on the joint effort of many people. We would like to thank all the authors who submitted papers, whether accepted or not. We would also like to thank the Program Committee members and additional reviewers, who volunteered their time to carefully evaluate the numerous submissions. In addition, we would like to thank the General Chair, Rob Cunningham, for handling the conference arrangements, Ari Trachtenberg for handling publication, Jon Giffin for publicizing the conference, Anup Ghosh for finding sponsors for the conference, and MIT Lincoln Lab for maintaining the conference website. Finally, we extend our thanks to The Institute for Information Infrastructure Protection (I3P), Symantec Corporation, IBM, and MIT Lincoln Laboratory for their sponsorship of student scholarships.

June 2008

Richard Lippmann
Engin Kirda

Organization

RAID 2008 was organized by MIT Lincoln Laboratory and held in conjunction with VIZSEC 2008.

Conference Chairs

Conference Chair	Robert Cunningham (MIT Lincoln Laboratory)
Program Chair	Richard Lippmann (MIT Lincoln Laboratory)
Program Co-chair	Engin Kirda (Eurecom / Technical University of Vienna)
Publications Chair	Ari Trachtenberg (Boston University)
Publicity Chair	Jon Giffin (Georgia Tech)
Sponsorship Chair	Anup Ghosh (George Mason University)

Program Committee

Michael Bailey	University of Michigan
Michael Behringer	Cisco
Herbert Bos	Vrije Universiteit
David Brumley	Carnegie Mellon University
Tzi-cker Chiueh	State University of New York at Stony Brook
Andrew Clark	Queensland University of Technology
Robert Cunningham	MIT Lincoln Lab
Ulrich Flegel	SAP Research
Debin Gao	Singapore Management University
Anup Ghosh	George Mason University
Jonathon Giffin	Georgia Institute of Technology
Thorsten Holz	University of Mannheim
Jaeyeon Jung	Intel
Engin Kirda	Institute Eurecom
Kwok-Yan Lam	Tsinghua University
Zhuowei Li	Microsoft
Richard Lippmann	MIT Lincoln Laboratory
Raffael Marty	Splunk
Benjamin Morin	Supélec
Rei Safavi-Naini	University of Calgary
R. Sekar	State University of New York at Stony Brook
Robin Sommer	ICSI and LBNL
Salvatore Stolfo	Columbia University
Toshihiro Tabata	Okayama University
Ari Trachtenberg	Boston University

VIII Organization

Vijay Varadharajan
Andreas Wespi
Diego Zamboni
Jianying Zhou

Macquarie University
IBM Zurich Research Laboratory
IBM Zurich Research Laboratory
Institute for Infocomm Research

Steering Committee

Marc Dacier (Chair)
Hervé Debar
Deborah Frinck
Ming-Yuh Huang
Erland Jonsson
Wenke Lee
Ludovic Mé
Alfonso Valdes
Giovanni Vigna
Andreas Wespi
S. Felix Wu
Diego Zamboni
Christopher Kruegel

EURECOM, France
France Télécom R&D, France
Pacific Northwest National Lab, USA
The Boeing Company, USA
Chalmers, Sweden
Georgia Tech, USA
Supélec, France
SRI International, USA
University of California, Santa Barbara, USA
IBM Research, Switzerland
UC Davis, USA
IBM Research, Switzerland
University of California, Santa Barbara, USA /
Technical University of Vienna, Austria

Additional Reviewers

Hirotake Abe
Manos Antonakakis
Venkat Balakrishnan
Ulrich Bayer
Leyla Bilge
Damiano Bolzoni
Gabriela Cretu
Italo Dacosta
Loic Dufлот
Thomas Dullien
Jose M. Fernandez
Vanessa Frias-Martinez
Jochen Haller
Philip Hendrix
Yoshiaki Hori
Kyle Ingols
Florian Kerschbaum
Hyung Chan Kim
Andreas Lang
Pavel Laskov
Timothy Leek

Toyohashi University of Technology
Georgia Tech
Macquarie University
Technical University of Vienna
Technical University of Vienna
University of Twente
Columbia University
Georgia Tech
DCSSI
Zynamics
École Polytechnique de Montréal
Columbia University
SAP Research
Harvard University
Kyushu University
MIT Lincoln Laboratory
SAP Research
Columbia University
University of Magdeburg
Fraunhofer FIRST & University of Tuebingen
MIT Lincoln Laboratory

Zhenkai Liang	National University of Singapore
Ludovic Mé	Supélec
Chee Meng	Tey
Philip Miseldine	SAP Research
Andreas Moser	Technical University of Vienna
Jon Oberhide	University of Michigan
Yoshihiro Oyama	The University of Electro-Communications
Yoshiaki Shiraishi	Nagoya Institute of Technology
Sushant Sinha	University of Michigan
Yingbo Song	Columbia University
Abhinav Srivastava	Georgia Tech
Eric Totel	Supélec
Uday Tupakula	Macquarie University
Shobha Venkataraman	CMU
Peter Wurzinger	Technical University of Vienna
Sachiko Yoshihama	IBM Tokyo Research Laboratory
Weiliang Zhao	Macquarie University

Sponsoring Institutions

The Institute for Information Infrastructure Protection (I3P)
Symantec Corporation
IBM
MIT Lincoln Laboratory

Table of Contents

Recent Advances in Intrusion Detection

Rootkit Prevention

Guest-Transparent Prevention of Kernel Rootkits with VMM-Based Memory Shadowing	1
<i>Ryan Riley, Xuxian Jiang, and Dongyan Xu</i>	
Countering Persistent Kernel Rootkits through Systematic Hook Discovery	21
<i>Zhi Wang, Xuxian Jiang, Weidong Cui, and Xinyuan Wang</i>	

Malware Detection and Prevention

Tamper-Resistant, Application-Aware Blocking of Malicious Network Connections	39
<i>Abhinav Srivastava and Jonathon Giffin</i>	
A First Step towards Live Botmaster Traceback	59
<i>Daniel Ramsbrock, Xinyuan Wang, and Xuxian Jiang</i>	
A Layered Architecture for Detecting Malicious Behaviors	78
<i>Lorenzo Martignoni, Elizabeth Stinson, Matt Fredrikson, Somesh Jha, and John C. Mitchell</i>	
A Study of the Packer Problem and Its Solutions	98
<i>Fanglu Guo, Peter Ferrie, and Tzi-cker Chiueh</i>	

High Performance Intrusion Detection and Evasion

Gnort: High Performance Network Intrusion Detection Using Graphics Processors	116
<i>Giorgos Vasiliadis, Spiros Antonatos, Michalis Polychronakis, Evangelos P. Markatos, and Sotiris Ioannidis</i>	
Predicting the Resource Consumption of Network Intrusion Detection Systems	135
<i>Holger Dreger, Anja Feldmann, Vern Paxson, and Robin Sommer</i>	
High-Speed Matching of Vulnerability Signatures	155
<i>Nabil Shear, David R. Albrecht, and Nikita Borisov</i>	

Web Application Testing and Evasion

Swarm Attacks against Network-Level Emulation/Analysis 175
Simon P. Chung and Aloysius K. Mok

Leveraging User Interactions for In-Depth Testing of Web Applications 191
Sean McAllister, Engin Kirda, and Christopher Kruegel

Model-Based Covert Timing Channels: Automated Modeling and Evasion 211
Steven Gianvecchio, Haining Wang, Duminda Wijesekera, and Sushil Jajodia

Alert Correlation and Worm Detection

Optimal Cost, Collaborative, and Distributed Response to Zero-Day Worms - A Control Theoretic Approach 231
Senthilkumar G. Cheetancheri, John-Mark Agosta, Karl N. Levitt, Felix Wu, and Jeff Rowe

On the Limits of Payload-Oblivious Network Attack Detection 251
M. Patrick Collins and Michael K. Reiter

Determining Placement of Intrusion Detectors for a Distributed Application through Bayesian Network Modeling 271
Gaspar Modelo-Howard, Saurabh Bagchi, and Guy Lebanon

A Multi-Sensor Model to Improve Automated Attack Detection 291
Magnus Almgren, Ulf Lindqvist, and Erland Jonsson

Anomaly Detection and Network Traffic Analysis

Monitoring SIP Traffic Using Support Vector Machines 311
Mohamed Nassar, Radu State, and Olivier Festor

The Effect of Clock Resolution on Keystroke Dynamics 331
Kevin Killourhy and Roy Maxion

A Comparative Evaluation of Anomaly Detectors under Portscan Attacks 351
Ayesha Binte Ashfaq, Maria Joseph Robert, Asma Mumtaz, Muhammad Qasim Ali, Ali Sajjad, and Syed Ali Khayam

Advanced Network Fingerprinting 372
Humberto J. Abdelnur, Radu State, and Olivier Festor

Posters

On Evaluation of Response Cost for Intrusion Response Systems (Extended Abstract)	390
<i>Natalia Stakhanova, Chris Strasburg, Samik Basu, and Johnny S. Wong</i>	
WebIDS: A Cooperative Bayesian Anomaly-Based Intrusion Detection System for Web Applications (Extended Abstract)	392
<i>Nathalie Dagorn</i>	
Evading Anomaly Detection through Variance Injection Attacks on PCA (Extended Abstract)	394
<i>Benjamin I.P. Rubinstein, Blaine Nelson, Ling Huang, Anthony D. Joseph, Shing-hon Lau, Nina Taft, and J.D. Tygar</i>	
Anticipating Hidden Text Salting in Emails (Extended Abstract)	396
<i>Christina Lioma, Marie-Francine Moens, Juan-Carlos Gomez, Jan De Beer, Andre Bergholz, Gerhard Paass, and Patrick Horkan</i>	
Improving Anomaly Detection Error Rate by Collective Trust Modeling (Extended Abstract)	398
<i>Martin Reháč, Michal Pěchouček, Karel Bartoš, Martin Grill, Pavel Čeleda, and Vojtěch Krmíček</i>	
Database Intrusion Detection and Response (Extended Abstract)	400
<i>Ashish Kamra and Elisa Bertino</i>	
An Empirical Approach to Identify Information Misuse by Insiders (Extended Abstract)	402
<i>Deanna D. Caputo, Greg Stephens, Brad Stephenson, Megan Cormier, and Minna Kim</i>	
Page-Based Anomaly Detection in Large Scale Web Clusters Using Adaptive MapReduce (Extended Abstract)	404
<i>Junsup Lee and Sungdeok Cha</i>	
Automating the Analysis of Honeypot Data (Extended Abstract)	406
<i>Olivier Thonnard, Jouni Viinikka, Corrado Leita, and Marc Dacier</i>	
Anomaly and Specification Based Cognitive Approach for Mission-Level Detection and Response (Extended Abstract)	408
<i>Paul Rubel, Partha Pal, Michael Atighetchi, D. Paul Benjamin, and Franklin Webber</i>	
Monitoring the Execution of Third-Party Software on Mobile Devices (Extended Abstract)	410
<i>Andrew Brown and Mark Ryan</i>	

Streaming Estimation of Information-Theoretic Metrics for Anomaly
Detection (Extended Abstract) 412
Sergey Bratus, Joshua Brody, David Kotz, and Anna Shubina

Bots Behaviors vs. Human Behaviors on Large-Scale Communication
Networks (Extended Abstract)..... 415
Wei Lu and Ali A. Ghorbani

Anomalous Taint Detection 417
Lorenzo Cavallaro and R. Sekar

Deep Packet Inspection Using Message Passing Networks
(Extended Abstract) 419
Divya Jain, K. Vasanta Lakshmi, and Priti Shankar

System Call API Obfuscation(Extended Abstract) 421
Abhinav Srivastava, Andrea Lanzi, and Jonathon Giffin

Author Index 423