Lecture Notes in Computer Science 5230

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

Springer

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

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

Vijay Varadharajan	Macquarie University
Andreas Wespi	IBM Zurich Research Laboratory
Diego Zamboni	IBM Zurich Research Laboratory
Jianying Zhou	Institute for Infocomm Research

Steering Committee

Marc Dacier (Chair)	EURECOM, France
Hervé Debar	France Télécom R&D, France
Deborah Frincke	Pacific Northwest National Lab, USA
Ming-Yuh Huang	The Boeing Company, USA
Erland Jonsson	Chalmers, Sweden
Wenke Lee	Georgia Tech, USA
Ludovic Mé	Supélec, France
Alfonso Valdes	SRI International, USA
Giovanni Vigna	University of California, Santa Barbara, USA
Andreas Wespi	IBM Research, Switzerland
S. Felix Wu	UC Davis, USA
Diego Zamboni	IBM Research, Switzerland
Christopher Kruegel	University of California, Santa Barbara, USA / Technical University of Vienna, Austria

Additional Reviewers

Hirotake Abe	Toyohashi University of Technology
Manos Antonakakis	Georgia Tech
Venkat Balakrishnan	Macquarie University
Ulrich Bayer	Technical University of Vienna
Leyla Bilge	Technical University of Vienna
Damiano Bolzoni	University of Twente
Gabriela Cretu	Columbia University
Italo Dacosta	Georgia Tech
Loic Duflot	DCSSI
Thomas Dullien	Zynamics
Jose M. Fernandez	École Polytechnique de Montréal
Vanessa Frias-Martinez	Columbia University
Jochen Haller	SAP Research
Philip Hendrix	Harvard University
Yoshiaki Hori	Kyushu University
Kyle Ingols	MIT Lincoln Laboratory
Florian Kerschbaum	SAP Research
Hyung Chan Kim	Columbia University
Andreas Lang	University of Magdeburg
Pavel Laskov	Fraunhofer FIRST & University of Tuebingen
Timothy Leek	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

Web Application Testing and Evasion

Alert Correlation and Worm Detection

Anomaly Detection and Network Traffic Analysis

Posters