Lecture Notes in Computer Science 5758

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

Engin Kirda Somesh Jha
Davide Balzarotti (Eds.)

Recent Advances in Intrusion Detection

12th International Symposium, RAID 2009
Saint-Malo, France, September 23-25, 2009
Proceedings

Volume Editors

Engin Kirda
Institute Eurecom
2229 Route des Cretes, 06560 Sophia-Antipolis Cedex, France
E-mail: engin.kirda@eurecom.fr

Somesh Jha
University of Wisconsin, Computer Sciences Department
Madison, WI 53706, USA
E-mail: jha@cs.wisc.edu

Davide Balzarotti
Institute Eurecom
2229 Route des Cretes, 06560 Sophia-Antipolis Cedex, France
E-mail: davide.balzarotti@eurecom.fr

Library of Congress Control Number: 2009934013

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 3-642-04341-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-04341-3 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12752768 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 12th International Symposium on Recent Advances in Intrusion Detection systems (RAID 2009), which took place in Saint-Malo, France, during September 23–25. As in the past, 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 research papers on anomaly and specification-based approaches, malware detection and prevention, network and host intrusion detection and prevention, intrusion detection for mobile devices, and high-performance intrusion detection. Furthermore, there was a poster session on emerging research areas and case studies.

The RAID 2009 Program Committee received 59 full paper submissions from all over the world. All submissions were carefully reviewed by independent reviewers on the basis of space, topic, technical assessment, and overall balance. The final selection took place at the Program Committee meeting on May 21 in Oakland, California. In all, 17 papers were selected for presentation and publication in the conference proceedings. As a continued feature, 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 posters were submitted for a numerical review by an independent, three-person sub-committee of the Program Committee based on novelty, description, and evaluation. The sub-committee recommended the acceptance of 16 of these posters for presentation and publication.

The success of RAID 2009 depended on the joint effort of many people. We would like to thank all the authors of submitted papers. We would also like to thank the Program Committee members and additional reviewers, who volunteered their time to evaluate the numerous submissions. In addition, we would like to thank the General Chair, Ludovic Me, for handling the conference arrangements, Davide Balzarotti, for handling the publication, Corrado Leita for publicizing the conference, Christophe Bidan for finding sponsors for the conference, and SUPELEC for hosting the conference website. We would also like to thank our sponsors, DCSSI, INRIA Grand Est, EADS, Alcatel Lucent and Fondation Michel Metivier.

July 2009

Engin Kirda
Somesh Jha

Organization

RAID 2009 was organized by SUPELEC and it was co-located with ESORICS 2009.

Conference Chairs

General Chair	Ludovic Mé (SUPELEC)
Program Chair	Engin Kirda (Eurecom)
Program Co-chair	Somesh Jha (University of Wisconsin)
Sponsorship Chair	Christophe Bidan (SUPELEC)
Publicity Chair	Corrado Leita (Symantec Research Europe)
Publications Chair	Davide Balzarotti (Eurecom)

Steering Committee

Marc Dacier	Symantec Research Europe
Robert Cunnigham	MIT Lincoln Laboratory, USA
Hervé Debar	France Telecom R&D, France
Deborah Frincke	Pacific Northwest National Lab, USA
Ming-Yuh Huang	The Boeing Company, USA
Erland Jonsson	Chalmers University, Sweden
Christopher Kruegel	University of California, Santa Barbara, USA
Wenke Lee	Georgia Tech, USA
Richard Lippmann	MIT Lincoln Laboratory
Ludovic Mé	SUPELEC, 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

Program Committee

Anil Somayaji	Carleton University, Canada
Benjamin Morin	Central Directorate for Information System Security, France
Christopher Kruegel	University of California, Santa Barbara, USA
Collin Jackson	Stanford University, USA
Corrado Leita	Symantec Research Europe, France
David Brumley	Carnegie Mellon University, USA
Davide Balzarotti	Eurecom, France

Dongyan Xu	Purdue University, USA
Engin Kirda	Eurecom, France
Giovanni Vigna	University of California, Santa Barbara, USA
Guevara Noubir	North Eastern University, USA
Guofei Gu	Texas A&M University, USA
Jaeyeon Jung	Intel Research, USA
John Viega	Stonewall Software, USA
Jonathan Giffin	Georgia Institute of Technology, USA
Jouni Viinikka	Orange Labs, France
Kathy Wang	MITRE, USA
Manuel Costa	Microsoft Research, Cambridge, UK
Michael Bailey	University of Michigan, USA
Mihai Christodorescu	IBM T.J. Watson Research Center, USA
Olivier Festor	INRIA, France
R. Sekar	Stoney Brook University, USA
Radu State	University of Luxembourg, Luxembourg
Robert Cunningham	MIT Lincoln Labs, USA
Robin Sommer	International Computer Science Institute, USA
Somesh Jha	University of Wisconsin, USA
Sotiris Ioannidis	FORTH, Greece
Thorsten Holz	University of Mannheim, Germany
Xuxian Jiang	North Carolina State University, USA

Additional Reviewers

Rémi Badonnel	INRIA, France
Adam Barth	UC Berkeley, USA
Drew Davidson	University of Wisconsin, USA
Matt Fredrickson	University of Wisconsin, USA
Zhiqiang Lin	Purdue University, USA
Daniel Luchaup	University of Wisconsin, USA
Roberto Perdisci	Damballa, Inc., USA
Ryan Riley	Purdue University, USA
Elizabeth Stinson	Stanford University, USA
Alok Tongoankar	Stony Brook University, USA
Zhi Wang	North Carolina State University, USA

Sponsoring Institutions

DCSSI (Direction centrale de la sécurité des systèmes d'information)

INRIA Grand Est

EADS

Alcatel Lucent

Fondation Michel Metivier

Table of Contents

Intrusion Detection for Mobile Devices

High-Performance Intrusion Detection

Malware Detection and Prevention (II)

Posters