Lecture Notes in Computer Science 6961

Robin Sommer Davide Balzarotti
Gregor Maier (Eds.)

Recent Advances in Intrusion Detection

14th International Symposium, RAID 2011
Menlo Park, CA, USA, September 20-21, 2011
Proceedings

Springer

Volume Editors

Robin Sommer
Gregor Maier
ICSI
1947 Center St, Ste 600, Berkeley, CA 94704, USA
E-mail: {robin, gregor}@icir.org

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

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-23643-3 e-ISBN 978-3-642-23644-0
DOI 10.1007/978-3-642-23644-0
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011935250

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

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

On behalf of the Program Committee, it is our pleasure to present the proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection Systems (RAID 2011), which took place in Menlo Park, California, during September 20-21, 2011. 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 eight technical sessions presenting full research papers on application security, malware, anomaly detection, network security, Web security and social networks, and sandboxing and embededed environments. Furthermore, there was a panel discussion on open-source network intrusion detection systems as well as a poster session presenting emerging research areas and case studies.

The RAID 2011 Program Committee received 87 full paper submissions from all over the world. All submissions were carefully reviewed by independent reviewers on the basis of technical quality, topic, space, and overall balance. The final decision took place at a Program Committee meeting on May 26 in Berkeley, California, where 20 papers were eventually selected for presentation at the conference and publication in the proceedings.

The success of RAID 2011 depended on the joint effort of many people. We would like to thank all the authors of submitted papers and posters. We would also like to thank the Program Committee members and additional reviewers, who volunteered their time to carefully evaluate all the submissions. Furthermore, we would like to thank the General Chair, Alfonso Valdes, for handling the conference arrangements; Gregor Maier for handling the publication process; Guofei Gu for publicizing the conference; the Communications Research Centre Canada for maintaining the conference website; and SRI International for hosting the conference.

September 2011

Robin Sommer
Davide Balzarotti

Organization

Organizing Committee

General Chair	Alfonso Valdes, SRI International, USA
Program Chair	Robin Sommer, ICSI / LBNL, USA
Program Co-Chair	Davide Balzarotti, Eurecom, France
Publication Chair	Gregor Maier, ICSI, USA
Publicity Chair	Guofei Gu, Texas A&M, USA

Program Committee

Michael Bailey	University of Michigan, USA
Elie Bursztein	Stanford University, USA
Juan Caballero	IMDEA Software, Spain
Michael Collins	RedJack, USA
Manuel Costa	Microsoft Research, UK
Marco Cova	University of Birmingham, UK
Holger Dreger	Siemens AG, Germany
Debin Gao	Singapore Management University, Singapore
Jonathan Giffin	Georgia Tech, USA
Guofei Gu	Texas A&M, USA
Guillaume Hiet	Supélec, France
Thorsten Holz	Ruhr University Bochum, Germany
Sotiris Ioannidis	FORTH, Greece
Jaeyeon Jung	Intel Labs Seattle, USA
Syed Ali Khayam	National University of Sciences and Technology (NUST), Pakistan
Christian Kreibich	ICSI, USA
Christopher Kruegel	UC Santa Barbara, USA
Corrado Leita	Symantec Research, France
Gregor Maier	ICSI, USA
Benjamin Morin	ANSSI, France
Phil Porras	SRI International, USA
William Robertson	UC Berkeley, USA
Anil Somayaji	Carleton University, Canada
Angelos Stavrou	George Mason University, USA
Charles Wright	MIT Lincoln Laboratory, USA

External Reviewers

Zahid Anwar
Leyla Bilge
Matt Bishop
Steven Cheung
Brendan Dolan-Gavitt
Manuel Egele
Chris Grier
Payas Gupta
Sharath Hiremangalore
Joshua Hodosh
Johannes Hoffmann
Ralf Hund
Engin Kirda
Marc Kührer
Andrea Lanzi
Meixing Le
Kangjie Lu
Seungwon Shin
Abhinav Srivastava
Gianluca Stringhini
Kurt Thomas
Sebastian Uellenbeck
Nicholas Weaver
Zhaoyan Xu
Chao Yang
Vinod Yegneswaran

Steering Committee

Chair

Marc Dacier	Eurecom, France

Members

Hervé Debar	Télécom SudParis, France
Deborah Frincke	National Security Agency, USA
Ming-Yuh Huang	The Boeing Company, USA
Somesh Jha	University of Wisconsin, USA
Erland Jonsson	Chalmers, Sweden
Engin Kirda	Northeastern University, USA
Christopher Kruegel	UC Santa Barbara, USA
Wenke Lee	Georgia Tech, USA
Richard Lippmann	MIT Lincoln Laboratory, USA
Ludovic Me	Supélec, France
Alfonso Valdes	SRI International, USA
Giovanni Vigna	UC Santa Barbara, USA
Andreas Wespi	IBM Research, Switzerland
S. Felix Wu	UC Davis, USA
Diego Zamboni	HP Enterprise Services, Mexico

Table of Contents

Application Security

Malware

Anomaly Detection

Network Security

Web Security and Social Networks

Sandboxing and Embedded Environments