Lecture Notes in Computer Science 7462

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

Davide Balzarotti Salvatore J. Stolfo
Marco Cova (Eds.)

Research in Attacks, Intrusions, and Defenses

15th International Symposium, RAID 2012
Amsterdam, The Netherlands, September 12-14, 2012
Proceedings

Springer

Volume Editors

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

Salvatore J. Stolfo
Columbia University
Department of Computer Science
1214 Amsterdam Avenue, M.C. 0401
New York, NY 10027-7003, USA
E-mail: sal@cs.columbia.edu

Marco Cova
University of Birmingham
School of Computer Science
Edgbaston, Birmingham, B15 2TT, UK
E-mail: m.cova@cs.bham.ac.uk

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-33337-8 e-ISBN 978-3-642-33338-5
DOI 10.1007/978-3-642-33338-5
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012946390

CR Subject Classification (1998): C.2.0, D.4.6, K.6.5, K.4.4, H.2.7, C.2, H.4, H.5.3

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 15th International Symposium on Research in Attacks, Intrusions, and Defenses (RAID 2012), which took place in Amsterdam, The Netherlands, during September 12–14, 2012.

For its 15th anniversary, the RAID symposium changed its name from "Recent Advances in Intrusion Detection" to "Research in Attacks, Intrusions and Defenses." The new name reflects the broader scope of the conference that now aims at bringing together leading researchers and practitioners from academia, government, and industry to discuss novel research contributions related to any area of computer and information security.

This year, there were six technical sessions presenting full research papers on virtualization security, attacks and defenses, host and network security, fraud detection and underground economy, Web security, and intrusion detection systems. Furthermore, there was an invited talk to present the most influential paper presented in the first five years of the RAID conference and a poster session presenting emerging research areas and case studies.

The RAID 2012 Program Committee received 84 full paper submissions from all over the world. All submissions were carefully reviewed by independent reviewers on the basis of technical quality, topic, novelty, and overall balance. The final decision took place at a Program Committee meeting on May 24 in San Francisco, California, where 18 papers were eventually selected for presentation at the conference and publication in the proceedings. The symposium also accepted 12 poster presentations, reporting early-stage research, demonstration of applications, or case studies. An extended abstract of each accepted poster is included in the proceedings.

The success of RAID 2012 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, Bruno Crispo, for handling the conference arrangements; Marco Cova for handling the publication process; William Robertson and Sotiris Ioannidis for publicizing the conference; Stefano Ortolani for maintaining the conference website and helping with the local arrangements; and the Vrije Universiteit in Amsterdam for hosting the conference. We would also like to thank our sponsor Symantec, for supporting the conference.

September 2012

Davide Balzarotti
Salvatore Stolfo

Organization

Organizing Committee

General Chair

Bruno Crispo	University of Trento, Italy

Program Chair

Davide Balzarotti	Eurecom, France

Program Co-chair

Salvatore Stolfo	Columbia University, USA

Publication Chair

Marco Cova	University of Birmingham, UK

Publicity Chairs

Sotiris Ioannidis	FORTH, Greece
William Robertson	Northeastern University, USA

Local Chair

Stefano Ortolani	Vrije Universiteit, The Netherlands

Program Committee

Anil Somayaji	Carleton University, Canada
Michael Bailey	University of Michigan, USA
Mihai Christodorescu	IBM T.J. Watson Research Center, USA
Juan Caballero	IMDEA Software Software Institute, Spain
Srdjan Capkun	ETH Zurich, Switzerland
Marco Cova	University of Birmingham, UK
Nick Feamster	Georgia Tech, USA
Debin Gao	Singapore Management University, Singapore
Guofei Gu	Texas A&M, USA
Guillaume Hiet	Supelec, France
Thorsten Holz	Ruhr University Bochum, Germany
Sotiris Ioannidis	FORTH, Greece
Gregor Maier	ICSI, USA

Christian Kreibich	ICSI, USA
Christopher Kruegel	UC Santa Barbara, USA
Andrea Lanzi	EURECOM, France
Corrado Leita	Symantec Research, France
Benjamin Livshits	Microsoft Research, USA
Fabian Monrose	University of North Carolina at Chapel Hill, USA
Benjamin Morin	ANSSI, France
Roberto Perdisci	University of Georgia, USA
William Robertson	Northeastern University, USA
Abhinav Srivastava	AT&T Labs-Research, USA
Angelos Stavrou	George Mason University, USA
Dongyan Xu	Purdue, USA
Charles Wright	MIT Lincoln Laboratory, USA

External Reviewers

Elias Athanasopoulos	Ryad Benadjila	Gehana Booth
Shakeel Butt	Zhui Deng	Zhongshu Gu
Amin Hassanzadeh	Sharath Hiremagalore	Johannes Hoffmann
George Kontaxis	Lazaros Koromilas	Kyu Hyung Lee
Zhiqiang Lin	Luc des trois Maisons	Saran Neti
Antonis Papadogiannakis	Fei Peng	Junghwan Rhee
R. Scott Robertson	Zacharias Tzermias	Pu Shi
Seungwon Shin	Dannie Stanley	George Vassiliadis
Tielei Wang	Zhaohui Wang	Chao Yang
Jialong Zhang		

Steering Committee

Chair

Marc Dacier	Symantec, USA

Members

Herve Debar	Telecom SudParis, France
Deborah Frincke	Pacific Northwest National Lab, USA
Ming-Yuh Huang	Northwest Security Institute, 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	Supelec, France
Robin Sommer	ICSI/LBNL, USA
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

Virtualization

Attacks and Defenses

Host and Network Security

Fraud Detection and Underground Economy

Web Security

Intrusion Detection

Poster Abstracts