

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

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

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

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

© Springer-Verlag Berlin Heidelberg 2011

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

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

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

Minemu: The World's Fastest Taint Tracker	1
<i>Erik Bosman, Asia Slowinska, and Herbert Bos</i>	
DYMO: Tracking Dynamic Code Identity	21
<i>Bob Gilbert, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna</i>	
Automated Identification of Cryptographic Primitives in Binary Programs	41
<i>Felix Gröbert, Carsten Willems, and Thorsten Holz</i>	

Malware

Shellzer: A Tool for the Dynamic Analysis of Malicious Shellcode	61
<i>Yanick Fratantonio, Christopher Kruegel, and Giovanni Vigna</i>	
KLIMAX: Profiling Memory Write Patterns to Detect Keystroke-Harvesting Malware	81
<i>Stefano Ortolani, Cristiano Giuffrida, and Bruno Crispo</i>	
Packed, Printable, and Polymorphic Return-Oriented Programming	101
<i>Kangjie Lu, Dabi Zou, Weiping Wen, and Debin Gao</i>	
On the Expressiveness of Return-into-libc Attacks	121
<i>Minh Tran, Mark Etheridge, Tyler Bletsch, Xuzian Jiang, Vincent Freeh, and Peng Ning</i>	

Anomaly Detection

Cross-Domain Collaborative Anomaly Detection: So Far Yet So Close	142
<i>Nathaniel Boggs, Sharath Hiremagalore, Angelos Stavrou, and Salvatore J. Stolfo</i>	
Revisiting Traffic Anomaly Detection Using Software Defined Networking	161
<i>Syed Akbar Mehdi, Junaid Khalid, and Syed Ali Khayam</i>	
Modeling User Search Behavior for Masquerade Detection	181
<i>Malek Ben Salem and Salvatore J. Stolfo</i>	

Network Security

Securing Application-Level Topology Estimation Networks: Facing the Frog-Boiling Attack	201
<i>Sheila Becker, Jeff Seibert, Cristina Nita-Rotaru, and Radu State</i>	
Detecting Traffic Snooping in Tor Using Decoys	222
<i>Sambuddho Chakravarty, Georgios Portokalidis, Michalis Polychronakis, and Angelos D. Keromytis</i>	
Cross-Analysis of Botnet Victims: New Insights and Implications	242
<i>Seungwon Shin, Raymond Lin, and Guofei Gu</i>	

Web Security and Social Networks

Banksafe Information Stealer Detection Inside the Web Browser	262
<i>Armin Buescher, Felix Leder, and Thomas Siebert</i>	
ICESHIELD: Detection and Mitigation of Malicious Websites with a Frozen DOM	281
<i>Mario Heiderich, Tilman Frosch, and Thorsten Holz</i>	
Spam Filtering in Twitter Using Sender-Receiver Relationship	301
<i>Jonghyuk Song, Sangho Lee, and Jong Kim</i>	
Die Free or Live Hard? Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers	318
<i>Chao Yang, Robert Chandler Harkreader, and Guofei Gu</i>	

Sandboxing and Embedded Environments

Detecting Environment-Sensitive Malware	338
<i>Martina Lindorfer, Clemens Kolbitsch, and Paolo Milani Comparetti</i>	
Defending Embedded Systems with Software Symbiotes	358
<i>Ang Cui and Salvatore J. Stolfo</i>	
What If You Can't Trust Your Network Card?	378
<i>Loïc Duflot, Yves-Alexis Perez, and Benjamin Morin</i>	

Author Index	399
---------------------------	-----