

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

University of Dortmund, 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 of Computer Science, Saarbruecken, Germany

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



Springer

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

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.

springer.com

© Springer-Verlag Berlin Heidelberg 2009

Printed in Germany

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 Cunningham	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

Recent Advances in Intrusion Detection Anomaly and Specification-Based Approaches

Panacea: Automating Attack Classification for Anomaly-Based Network Intrusion Detection Systems	1
<i>Damiano Bolzoni, Sandro Etalle, and Pieter H. Hartel</i>	
Protecting a Moving Target: Addressing Web Application Concept Drift	21
<i>Federico Maggi, William Robertson, Christopher Kruegel, and Giovanni Vigna</i>	
Adaptive Anomaly Detection via Self-calibration and Dynamic Updating	41
<i>Gabriela F. Cretu-Ciocarlie, Angelos Stavrou, Michael E. Locasto, and Salvatore J. Stolfo</i>	
Runtime Monitoring and Dynamic Reconfiguration for Intrusion Detection Systems	61
<i>Martin Rehák, Eugen Staab, Volker Fusenig, Michal Pěchouček, Martin Grill, Jan Stiborek, Karel Bartoš, and Thomas Engel</i>	

Malware Detection and Prevention (I)

Malware Behavioral Detection by Attribute-Automata Using Abstraction from Platform and Language	81
<i>Grégoire Jacob, Hervé Debar, and Eric Filiol</i>	
Automatic Generation of String Signatures for Malware Detection	101
<i>Kent Griffin, Scott Schneider, Xin Hu, and Tzi-cker Chiueh</i>	
PE-Miner: Mining Structural Information to Detect Malicious Executables in Realtime	121
<i>M. Zubair Shafiq, S. Momina Tabish, Fauzan Mirza, and Muddassar Farooq</i>	

Network and Host Intrusion Detection and Prevention

Automatically Adapting a Trained Anomaly Detector to Software Patches	142
<i>Peng Li, Debin Gao, and Michael K. Reiter</i>	
Towards Generating High Coverage Vulnerability-Based Signatures with Protocol-Level Constraint-Guided Exploration	161
<i>Juan Caballero, Zhenkai Liang, Pongsin Poosankam, and Dawn Song</i>	

Automated Behavioral Fingerprinting 182
Jérôme François, Humberto AbdeInur, Radu State, and Olivier Festor

Intrusion Detection for Mobile Devices

SMS-Watchdog: Profiling Social Behaviors of SMS Users for Anomaly Detection	202
<i>Guanhua Yan, Stephan Eidenbenz, and Emanuele Galli</i>	

Keystroke-Based User Identification on Smart Phones 224
*Saira Zahid, Muhammad Shahzad, Syed Ali Khayam, and
Muddassar Farooq*

VirusMeter: Preventing Your Cellphone from Spies 244
Lei Liu, Guanhua Yan, Xinwen Zhang, and Songqing Chen

High-Performance Intrusion Detection

Regular Expression Matching on Graphics Hardware for Intrusion Detection	265
<i>Giorgos Vasiliadis, Michalis Polychronakis, Spiros Antonatos, Evangelos P. Markatos, and Sotiris Ioannidis</i>	

Multi-byte Regular Expression Matching with Speculation 284
Daniel Luchaup, Randy Smith, Cristian Estan, and Somesh Jha

Malware Detection and Prevention (II)

Toward Revealing Kernel Malware Behavior in Virtual Execution
Environments 304
Chaoting Xuan, John Copeland, and Raheem Beyah

Exploiting Temporal Persistence to Detect Covert Botnet Channels 326
*Frederic Giroire, Jaideep Chandrashekar, Nina Taft,
 Eve Schooler, and Dina Papagiannaki*

Posters

An Experimental Study on Instance Selection Schemes for Efficient
Network Anomaly Detection..... 346
Yang Li, Li Guo, Bin-Xing Fang, Xiang-Tao Liu, and Lin-Qi

Automatic Software Instrumentation for the Detection of
Non-control-data Attacks 348
Jonathan-Christofer Demay, Éric Totel, and Frédéric Tronel

BLADE: Slashing the Invisible Channel of Drive-by Download Malware	350
<i>Long Lu, Vinod Yegneswaran, Phillip Porras, and Wenke Lee</i>	
CERN Investigation of Network Behaviour and Anomaly Detection	353
<i>Milosz Marian Hulboj and Ryszard Erazm Jurga</i>	
Blare Tools: A Policy-Based Intrusion Detection System Automatically Set by the Security Policy	355
<i>Laurent George, Valérie Viet Triem Tong, and Ludovic Mé</i>	
Detection, Alert and Response to Malicious Behavior in Mobile Devices: Knowledge-Based Approach	357
<i>Asaf Shabtai, Uri Kanonov, and Yuval Elovici</i>	
Autonomic Intrusion Detection System	359
<i>Wei Wang, Thomas Guyet, and Svein J. Knapskog</i>	
ALICE@home: Distributed Framework for Detecting Malicious Sites	362
<i>Ikpeme Erete, Vinod Yegneswaran, and Phillip Porras</i>	
Packet Space Analysis of Intrusion Detection Signatures	365
<i>Frédéric Massicotte</i>	
Traffic Behaviour Characterization Using NetMate	367
<i>Annie De Montigny-Leboeuf, Mathieu Couture, and Frederic Massicotte</i>	
On the Inefficient Use of Entropy for Anomaly Detection	369
<i>Mobin Javed, Ayesha Binte Ashfaq, M. Zubair Shafiq, and Syed Ali Khayam</i>	
Browser-Based Intrusion Prevention System	371
<i>Ikpeme Erete</i>	
Using Formal Grammar and Genetic Operators to Evolve Malware	374
<i>Sadia Noreen, Shafaq Murtaza, M. Zubair Shafiq, and Muddassar Farooq</i>	
Method for Detecting Unknown Malicious Executables	376
<i>Boris Rozenberg, Ehud Gudes, Yuval Elovici, and Yuval Fledel</i>	
Brave New World: Pervasive Insecurity of Embedded Network Devices	378
<i>Ang Cui, Yingbo Song, Pratap V. Prabhu, and Salvatore J. Stolfo</i>	
DAEDALUS: Novel Application of Large-Scale Darknet Monitoring for Practical Protection of Live Networks (Extended Abstract)	381
<i>Daisuke Inoue, Mio Suzuki, Masashi Eto, Katsunari Yoshioka, and Koji Nakao</i>	
Author Index	383