

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

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

© Springer-Verlag Berlin Heidelberg 2012

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 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
William Robertson

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

VIII Organization

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 Monroe	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

Trusted VM Snapshots in Untrusted Cloud Infrastructures	1
<i>Abhinav Srivastava, Himanshu Raj, Jonathon Giffin, and Paul England</i>	
Secure and Robust Monitoring of Virtual Machines through Guest-Assisted Introspection	22
<i>Martim Carbone, Matthew Conover, Bruce Montague, and Wenke Lee</i>	
Assessing the Trustworthiness of Drivers	42
<i>Shengzhi Zhang and Peng Liu</i>	

Attacks and Defenses

Industrial Espionage and Targeted Attacks: Understanding the Characteristics of an Escalating Threat	64
<i>Olivier Thonnard, Leyla Bilge, Gavin O’Gorman, Seán Kiernan, and Martin Lee</i>	
Memory Errors: The Past, the Present, and the Future	86
<i>Victor van der Veen, Nitish dutt-Sharma, Lorenzo Cavallaro, and Herbert Bos</i>	
A Memory Access Validation Scheme against Payload Injection Attacks	107
<i>Dongkyun Ahn and Gyungho Lee</i>	

Host and Network Security

DIONE: A Flexible Disk Monitoring and Analysis Framework	127
<i>Jennifer Mankin and David Kaeli</i>	
AK-PPM: An Authenticated Packet Attribution Scheme for Mobile Ad Hoc Networks	147
<i>Zhi Xu, Hungyuan Hsu, Xin Chen, Sencun Zhu, and Ali R. Hurson</i>	

Fraud Detection and Underground Economy

Paying for Piracy? An Analysis of One-Click Hosters’ Controversial Reward Schemes	169
<i>Tobias Lauinger, Engin Kirda, and Pietro Michiardi</i>	

Proactive Discovery of Phishing Related Domain Names	190
<i>Samuel Marchal, Jérôme François, Radu State, and Thomas Engel</i>	
Evaluating Electricity Theft Detectors in Smart Grid Networks	210
<i>Daisuke Mashima and Alvaro A. Cárdenas</i>	

Web Security

PoisonAmplifier: A Guided Approach of Discovering Compromised Websites through Reversing Search Poisoning Attacks	230
<i>Jialong Zhang, Chao Yang, Zhaoyan Xu, and Guofei Gu</i>	
DEMACRO: Defense against Malicious Cross-Domain Requests	254
<i>Sebastian Lekies, Nick Nikiforakis, Walter Tighzert, Frank Piessens, and Martin Johns</i>	
FlashDetect: ActionScript 3 Malware Detection	274
<i>Timon Van Overveldt, Christopher Kruegel, and Giovanni Vigna</i>	

Intrusion Detection

ALERT-ID: Analyze Logs of the Network Element in Real Time for Intrusion Detection	294
<i>Jie Chu, Zihui Ge, Richard Huber, Ping Ji, Jennifer Yates, and Yung-Chao Yu</i>	
A Lone Wolf No More: Supporting Network Intrusion Detection with Real-Time Intelligence	314
<i>Johanna Amann, Robin Sommer, Aashish Sharma, and Seth Hall</i>	
GPP-Grep: High-Speed Regular Expression Processing Engine on General Purpose Processors	334
<i>Victor C. Valgenti, Jatin Chhugani, Yan Sun, Nadathur Satish, Min Sik Kim, Changkyu Kim, and Pradeep Dubey</i>	
N-Gram against the Machine: On the Feasibility of the N-Gram Network Analysis for Binary Protocols	354
<i>Dina Hadziosmanović, Lorenzo Simionato, Damiano Bolzoni, Emmanuele Zambon, and Sandro Etalle</i>	

Poster Abstracts

Online Social Networks, a Criminals Multipurpose Toolbox (Poster Abstract)	374
<i>Shah Mahmood and Yvo Desmedt</i>	

The Triple-Channel Model: Toward Robust and Efficient Advanced Botnets (Poster Abstract)	376
<i>Cui Xiang, Shi Jinqiao, Liao Peng, and Liu Chaoge</i>	
Network Security Analysis Method Taking into Account the Usage Information (Poster Abstract)	378
<i>Wu Jinyu, Yin Lihua, and Fang Binxing</i>	
Automatic Covert Channel Detection in Asbestos System (Poster Abstract)	380
<i>Shuyuan Jin, Zhi Yang, and Xiang Cui</i>	
EFA for Efficient Regular Expression Matching in NIDS (Poster Abstract)	382
<i>Dengke Qiao, Tingwen Liu, Yong Sun, and Li Guo</i>	
Distress Detection (Poster Abstract)	384
<i>Mark Vella, Sotirios Terzis, and Marc Roper</i>	
Trie Data Structure to Compare Traffic Payload in a Supervised Anomaly Detection System (Poster Abstract)	386
<i>Jenny Andrea Pinto Sánchez and Luis Javier García Villalba</i>	
Towards Automated Forensic Event Reconstruction of Malicious Code (Poster Abstract)	388
<i>Ahmed F. Shosha, Joshua I. James, Chen-Ching Liu, and Pavel Gladyshev</i>	
Accurate Recovery of Functions in a Retargetable Decompiler (Poster Abstract)	390
<i>Lukáš Ďurфина, Jakub Křoustek, Petr Zemek, and Břetislav Kábele</i>	
Improvement of an Anagram Based NIDS by Reducing the Storage Space of Bloom Filters (Poster Abstract)	393
<i>Hugo Villanúa Vega, Jorge Maestre Vidal, Jaime Daniel Mejía Castro, and Luis Javier García Villalba</i>	
Concurrency Optimization for NIDS (Poster Abstract)	395
<i>Jorge Maestre Vidal, Hugo Villanúa Vega, Jaime Daniel Mejía Castro, and Luis Javier García Villalba</i>	
Malware Detection System by Payload Analysis of Network Traffic (Poster Abstract)	397
<i>Luis Javier García Villalba, Jaime Daniel Mejía Castro, Ana Lucila Sandoval Orozco, and Javier Martínez Puentes</i>	
Author Index	399