Lecture Notes in Computer Science 5137

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

Diego Zamboni (Ed.)

Detection of Intrusions and Malware, and Vulnerability Assessment

5th International Conference, DIMVA 2008
Paris, France, July 10-11, 2008
Proceedings

Springer

Volume Editor

Diego Zamboni
IBM Zurich Research Laboratory
Säumerstr. 4, 8803 Rüschlikon, Switzerland
E-mail: dza@zurich.ibm.com

Library of Congress Control Number: 2008930154

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-70541-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-70541-3 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12326570 06/3180 5 4 3 2 1 0

Preface

On behalf of the Program Committee, it is my pleasure to present the proceedings of the 5th GI International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA).

Every year since 2004 DIMVA has brought together leading researchers and practitioners from academia, government and industry to present and discuss novel security research. DIMVA is organized by the Security–Intrusion Detection and Response (SIDAR) special interest group of the German Informatics Society (GI).

The DIMVA 2008 Program Committee received 42 submissions from 16 different countries, and from governmental, industrial and academic organizations. All the submissions were carefully reviewed by several members of the Program Committee and evaluated on the basis of scientific novelty, importance to the field and technical quality. The final selection took place at the Program Committee meeting held on March 28, 2008 at the IBM Zürich Research Laboratory in Switzerland. Thirteen full papers and one extended abstract were selected for presentation and publication in the conference proceedings.

The conference took place during July 10-11, 2008, in the France Télécom R&D/Orange Labs premises of Issy les Moulineaux, near Paris, France, with the program grouped into five sessions. Two keynote speeches were presented by Richard Bejtlich (Director of Incident Response, General Electric) and by Tal Garfinkel (VMware Inc./Stanford University). The conference program also included a rump session organized by Sven Dietrich of the Stevens Institute of Technology, in which recent research results, works in progress, and other topics of interest to the community were presented.

A successful conference is the result of the joint effort of many people. In particular, I would like to thank all the authors who submitted papers, whether accepted or not. I also thank the Program Committee members and additional reviewers for their hard work in evaluating the submissions. In addition, I want to thank the General Chair, Hervé Debar from France Télécom R&D, for handling the conference arrangements and website, Tadeusz Pietraszek from Google for publicizing the conference, and Ludovic Mé from Supélec for finding sponsor support. Finally, I would like to express our gratitude to Google and EADS for their financial sponsorship.

July 2008 Diego Zamboni

Organization

Organizing Committee

General Chair	Hervé Debar, France Télécom R&D, France
Program Chair	Diego Zamboni, IBM Zürich Research Laboratory, Switzerland
Sponsor Chair	Ludovic Mé, Supélec, France
Publicity Chair	Tadeusz Pietraszek, Google, Switzerland

Program Committee

Kostas Anagnostakis	Institute for Infocomm Research, Singapore
Thomas Biege	SuSE, Germany
David Brumley	Carnegie Mellon University, USA
Roland Büschkes	RWE AG, Germany
Weidong Cui	Microsoft Research, USA
Marc Dacier	Institut Eurecom, France
Sven Dietrich	Stevens Institute of Technology, USA
Holger Dreger	Siemens CERT, Germany
Ulrich Flegel	SAP Research, Germany
Marc Heuse	Baseline Security Consulting, Germany
Thorsten Holz	University of Mannheim, Germany
Ming-Yuh Huang	Boeing, USA
Bernhard Hämmerli	HTA Lucerne, Switzerland
Martin Johns	University of Hamburg, Germany
Erland Jonsson	Chalmers University, Sweden
Klaus Julisch	IBM Zurich Research Laboratory, Switzerland
Christian Kreibich	International Computer Science Institute, USA
Christopher Kruegel	Technical University of Vienna, Austria
Pavel Laskov	Fraunhofer FIRST and University of Tübingen, Germany
Wenke Lee	Georgia Institute of Technology, USA
John McHugh	Dalhousie University, Canada
Michael Meier	University of Dortmund, Germany
Ludovic Mé	Supélec, France
John Mitchell	Stanford University, USA
George Mohay	Queensland University of Technology, Australia
Benjamin Morin	Supélec, France
Tadeusz Pietraszek	Google, Switzerland
Phil Porras	SRI International, USA
Stelios Sidiroglou	Columbia University, USA
Robin Sommer	ICSI/LBNL, USA
Morton Swimmer	City University of New York, USA
Peter Szor	Symantec, USA

Additional Reviewers

Christopher Alm	Wolfgang John	Carsten Willems
Vika Felmetsger	Henry Stern	Yves Younan
Felix Freiling	Elizabeth Stinson	Jacob Zimmermann

Steering Committee

Chairs	Ulrich Flegel (SAP Research)
	Michael Meier (University of Dortmund)
Members	Roland Büschkes (RWE AG)
	Marc Heuse (Baseline Security Consulting)
	Bernhard Hämmerli (HTA Lucerne)
	Klaus Julisch (IBM Zürich Research Laboratory)
	Christopher Kruegel (Technical University of Vienna)
	Pavel Laskov (Fraunhofer FIRST and University of Tübingen)
	Robin Sommer (ICSI/LBNL)

DIMVA 2008 was organized by the Special Interest Group Security — Intrusion Detection and Response (SIDAR) of the German Informatics Society (GI).

Support

Financial sponsorship for DIMVA 2008 was provided by Google (Gold Sponsor) and by EADS. We sincerely thank them for their support.

Table of Contents

Attack Prevention

Data Space Randomization 1
Sandeep Bhatkar and R. Sekar

XSS-GUARD: Precise Dynamic Prevention of Cross-Site Scripting Attacks 23
Prithvi Bisht and V.N. Venkatakrishnan

VeriKey: A Dynamic Certificate Verification System for Public Key Exchanges 44
Brett Stone-Gross, David Sigal, Rob Cohn, John Morse, Kevin Almeroth, and Christopher Kruegel

Malware Detection and Prevention (I)

Dynamic Binary Instrumentation-Based Framework for Malware Defense 64
Najwa Aaraj, Anand Raghunathan, and Niraj K. Jha

Embedded Malware Detection Using Markov n-Grams 88
M. Zubair Shafiq, Syed Ali Khayam, and Muddassar Farooq

Learning and Classification of Malware Behavior 108
Konrad Rieck, Thorsten Holz, Carsten Willems, Patrick Düssel, and Pavel Laskov

Attack Techniques and Vulnerability Assessment

On Race Vulnerabilities in Web Applications 126
Roberto Paleari, Davide Marrone, Danilo Bruschi, and Mattia Monga

On the Limits of Information Flow Techniques for Malware Analysis and Containment 143
Lorenzo Cavallaro, Prateek Saxena, and R. Sekar

Malware Detection and Prevention (II)

Expanding Malware Defense by Securing Software Installations 164
Weiqing Sun, R. Sekar, Zhenkai Liang, and V.N. Venkatakrishnan

FluXOR: Detecting and Monitoring Fast-Flux Service Networks 186
Emanuele Passerini, Roberto Paleari, Lorenzo Martignoni, and Danilo Bruschi

Traffic Aggregation for Malware Detection 207
Ting-Fang Yen and Michael K. Reiter

Intrusion Detection and Activity Correlation

The Contact Surface: A Technique for Exploring Internet Scale Emergent Behaviors 228
Carrie Gates and John McHugh

The Quest for Multi-headed Worms 247
Van-Hau Pham, Marc Dacier, Guillaume Urvoy-Keller, and Taoufik En-Najjary

A Tool for Offline and Live Testing of Evasion Resilience in Network Intrusion Detection Systems (Extended Abstract) 267
Leo Juan, Christian Kreibich, Chih-Hung Lin, and Vern Paxson

Author Index 279