Lecture Notes in Computer Science 5587

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

Ulrich Flegel Danilo Bruschi (Eds.)

Detection of Intrusions and Malware, and Vulnerability Assessment

6th International Conference, DIMVA 2009
Como, Italy, July 9-10, 2009
Proceedings

Springer

Volume Editors

Ulrich Flegel
SAP Research Center Karlsruhe
Karlsruhe, Germany
E-mail: ulrich.flegel@sap.com

Danilo Bruschi
Università degli Studi di Milano
Dipartimento di Informatica e Comunicazione
Milano, Italy
E-mail: bruschi@dico.unimi.it

Library of Congress Control Number: Applied for

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 3-642-02917-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-02917-2 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12716173 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 6th GI International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA).

Since 2004, DIMVA annually brings together leading researchers and practitioners from academia, government and industry to present and discuss novel security research. DIMVA is organized by the Special Interest Group *Security—Intrusion Detection and Response* (SIDAR)—of the German Informatics Society (GI).

The DIMVA 2009 Program Committee received 44 submissions from industrial and academic organizations from 17 different countries. Each submission was carefully reviewed by at least three Program Committee members or external experts. The submissions were 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 23, 2009, in Brussels, Belgium. Ten full papers and three extended abstracts were selected for presentation and publication in the conference proceedings.

The conference took place during July 9–10, 2009, at Villa Gallia, Lake Como, Italy, with the program grouped into five sessions. Two keynote speeches were presented by Richard A. Kemmerer (University of California, Santa Barbara) and Henry Stern (Ironport / Cisco). The conference program was complemented by the Capture-the-Flag contest CIPHER (Challenges in Informatics: Programming, Hosting and ExploRing) organized by Lexi Pimenidis (iDev GmbH) and a rump session organized by Sven Dietrich (Stevens Institute of Technology).

A successful conference is the result of the joint effort of many people. In particular, we would like to thank all the authors who submitted contributions. We also thank the Program Committee members and the additional reviewers for their hard work and diligent evaluation of the submissions. In addition we thank Thorsten Holz (University of Mannheim) for sponsor arrangements and Sebastian Schmerl (Technical University of Cottbus) for advertising the conference.

July 2009

Ulrich Flegel
Danilo Bruschi

Organization

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

Organizing Committee

General Chair	Danilo M. Bruschi, Università degli Studi di Milano, Italy
Program Chair	Ulrich Flegel, SAP Research
Rump Session Chair	Sven Dietrich, Stevens Institute of Technology, USA
Sponsorship Chair	Thorsten Holz, University of Mannheim, Germany
Publicity Chair	Sebastian Schmerl, Technical University of Cottbus, Germany

Program Committee

Thomas Biege	Novell, Germany
Gunter Bitz	SAP AG, Germany
Herbert Bos	Vrije Universiteit Amsterdam, The Netherlands
Danilo Bruschi	Università degli Studi di Milano, Italy
Roland Büschkes	RWE IT, Germany
Marc Dacier	Symantec Research Labs Europe, France
Hervé Debar	France Télécom R&D, France
Sven Dietrich	Stevens Institute of Technology, USA
Toralv Dirro	McAfee Avert Labs, Germany
Thomas Dullien	Zynamics, Germany
Bernhard Hämmerli	Acris GmbH and HSLU Lucerne, Switzerland
Marc Heuse	Baseline Security Consulting, Germany
Thorsten Holz	University of Mannheim, Germany
Erland Jonsson	Chalmers University of Technology, Sweden
Klaus Julisch	IBM Zurich Research Laboratory, Switzerland
Engin Kirda	Eurecom, France
Christian Kreibich	International Computer Science Institute, USA
Christopher Kruegel	UC Santa Barbara, USA
Pavel Laskov	University of Tuebingen, Germany
Wenke Lee	Georgia Institute of Technology, USA
Javier Lopez	University of Malaga, Spain

John McHugh	UNC and Dalhousie University, Canada
Michael Meier	Technical University of Dortmund, Germany
George Mohay	Queensland University of Technology, Australia
Martin Rehák	Czech Technical University in Prague, Czech Republic
Konrad Rieck	Berlin Institute of Technology, Germany
Sebastian Schmerl	BTU-Cottbus, Germany
Robin Sommer	ICSI/LBNL, USA
Salvatore Stolfo	Columbia University, USA
Peter Szor	Symantec Corporation, USA
Bernhard Thurm	SAP Research, Germany
Al Valdes	SRI International, USA

Additional Reviewers

Martin Apel	Christian Gehl	Lorenzo Martignoni
Marco Balduzzi	Cristian Grozea	Tomas Olovsson
Ulrich Bayer	Grégoire Jacob	Emanuele Passerini
Armin Büscher	Wolfgang John	Pratap Prabhu
Patrick Duessel	Matthias Kohler	Guido Schwenk
Manuel Egele	Tammo Krueger	Asia Slowinska

Steering Committee

Chairs	Ulrich Flegel, SAP Research
	Michael Meier, Technical University of Dortmund, Germany
Members	Roland Büschkes, RWE IT
	Hervé Debar, France Télécom R & D, France
	Bernhard Hämmerli, Acris GmbH and HSLU Lucerne, Switzerland
	Marc Heuse, Baseline Security Consulting
	Klaus Julisch, IBM Zurich Research Lab, Switzerland
	Christopher Kruegel, UC Santa Barbara, USA
	Pavel Laskov, University of Tuebingen, Germany
	Robin Sommer, ICSI/LBNL
	Diego Zamboni, IBM Zurich Research Lab, Switzerland

Table of Contents

Malware and SPAM

Emulation-Based Detection

Software Diversity

Harnessing Context

Anomaly Detection