Lecture Notes in Computer Science 6739

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

Thorsten Holz Herbert Bos (Eds.)

Detection of Intrusions and Malware, and Vulnerability Assessment

8th International Conference, DIMVA 2011
Amsterdam, The Netherlands, July 7-8, 2011
Proceedings

Springer

Volume Editors

Thorsten Holz
Ruhr-Universität Bochum
Fakultät für Elektrotechnik und Informationtechnik
AG "Embedded Malware"
Universitätsstrasse 150, 44801 Bochum, Germany
Email: thorsten.holz@rub.de

Herbert Bos
Vrije Universiteit Amsterdam
Computer Systems Section
1081 HV Amsterdam, The Netherlands
E-mail: herbertb@cs.vu.nl

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-22423-2 e-ISBN 978-3-642-22424-9
DOI 10.1007/978-3-642-22424-9
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011930927

CR Subject Classification (1998): C.2, K.6.5, D.4.6, E.3, H.4, K.4.4

LNCS Sublibrary: SL 4 – Security and Cryptology

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 to you the proceedings of the 8th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2011). Each year DIMVA brings together international experts from academia, industry and government 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 2011 Program Committee received 41 submissions. All submissions were carefully reviewed by at least three Program Committee members or external experts. The submissions were evaluated according to the criteria of scientific novelty, importance to the field and technical quality. The final selection took place at a Program Commitee meeting held on March 25, 2011, at Ruhr-University Bochum, Germany. Eleven full papers and two short papers were selected for presentation at the conference and publication in the conference proceedings. The conference took place during July 7-8, 2011, at Vrije Universiteit Amsterdam, The Netherlands. The program featured both practical and theoretical research results grouped into five sessions. The keynote speech was given by Manuel Costa, Microsoft Research. Another invited talk was presented by Ahmad-Reza Sadeghi, TU Darmstadt. The conference program further included a poster session.

We sincerely thank all those who submitted papers and posters as well as the Program Committee members and our external reviewers for their valuable contributions to a great conference program. In addition we thank Marc Kührer for helping during the preparation of these proceedings. For further details about DIMVA 2011, please refere to the conference website at http://www.dimva.org/dimva2011.

July 2011

Thorsten Holz
Herbert Bos

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	Herbert Bos, Vrije Universiteit Amsterdam, The Netherlands
Program Chair	Thorsten Holz, Ruhr-University Bochum, Germany
Sponsoring Chair	Damiano Bolzoni, University of Twente, The Netherlands
Publicity Chairs	Damiano Bolzoni, University of Twente, The Netherlands
	Konrad Rieck, TU Berlin, Germany
Local Chair	Asia Slowinska, Vrije Universiteit Amsterdam, The Netherlands
Workshops Chair	Lorenzo Cavallaro, Vrije Universiteit Amsterdam, The Netherlands

Program Committee

Michael Bailey	University of Michigan, USA
Herbert Bos	Vrije Universiteit Amsterdam, The Netherlands
Juan Caballero	IMDEA Software, Spain
Lorenzo Cavallaro	Vrije Universiteit Amsterdam, The Netherlands
Marco Cova	University of Birmingham, UK
Sven Dietrich	Stevens Institute of Technology, USA
Ulrich Flegel	Offenburg University of Applied Sciences, Germany
Felix Freiling	University of Erlangen-Nuremberg, Germany
Thorsten Holz	Ruhr-University Bochum, Germany
Martin Johns	SAP Research, Germany
Engin Kirda	Eurecom, France
Christian Kreibich	International Computer Science Institute, USA
Christopher Kruegel	University of California, Santa Barbara, USA
Pavel Laskov	University of Tübingen, Germany
Wenke Lee	Georgia Institute of Technology, USA
Corrado Leita	Symantec Research Labs, France
Lorenzo Martignoni	University of California, Berkeley, USA

Michael Meier	Technical University of Dortmund, Germany
Paolo Milani Comparetti	Vienna University of Technology, Austria
Konrad Rieck	TU Berlin, Germany
Robin Sommer	ICSI/LBNL, USA
Dongyan Xu	Purdue University, USA

Additional Reviewers

Zinaida Benenson	Achim D. Brucker	Andreas Dewald
Christian Dietrich	Hans-Georg Eßer	Jan Göbel
Mathias Kohler	Tammo Krüger	Zhiqiang Lin
Christian Moch	Tilo Müller	Lexi Pimenidis
Sebastian Schinzel	Thomas Schreck	Guido Schwenk
Moritz Steiner	Benjamin Stock	Carsten Willems

Steering Committee

Chairs	Ulrich Flegel, Offenburg University of Applied Sciences, Germany
	Michael Meier, Technical University of Dortmund, Germany
Members	Roland Büschkes, RWE AG, Germany
	Danilo M. Bruschi, Università degli Studi di Milano, Italy
	Herve Debar, France Telecom R&D, France
	Bernhard Haemmerli, Acris GmbH & HSLU Lucerne, Switzerland
	Marc Heuse, Baseline Security Consulting, Germany
	Marko Jahnke, Fraunhofer FKIE, Germany
	Klaus Julisch, IBM Zurich Research Lab, Switzerland
	Christian Kreibich, International Computer Science Institute, USA
	Christopher Kruegel, UC Santa Barbara, USA
	Pavel Laskov, University of Tübingen, Germany
	Robin Sommer, ICSI/LBNL, USA
	Diego Zamboni, IBM Zurich Research Lab, Switzerland

Table of Contents

Network Security I

Attacks

Web Security

Network Security II

Host Security