

*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*

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

*Massachusetts Institute of Technology, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Moshe Y. Vardi

*Rice University, Houston, TX, USA*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

Roland Büschkes Pavel Laskov (Eds.)

# Detection of Intrusions and Malware & Vulnerability Assessment

Third International Conference, DIMVA 2006  
Berlin, Germany, July 13-14, 2006  
Proceedings



Springer

## Volume Editors

Roland Büschkes  
RWE AG  
Opernplatz 1, 45128 Essen  
Germany  
E-mail: roland.bueschkes@rwe.com

Pavel Laskov  
Fraunhofer FIRST  
Kekuléstr. 7, 12489 Berlin, Germany  
E-mail: pavel.laskov@first.fraunhofer.de

Library of Congress Control Number: 2006928329

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	3-540-36014-X Springer Berlin Heidelberg New York
ISBN-13	978-3-540-36014-8 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 is a part of Springer Science+Business Media

[springer.com](http://springer.com)

© Springer-Verlag Berlin Heidelberg 2006  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper      SPIN: 11790754      06/3142      5 4 3 2 1 0

# Preface

On behalf of the Program Committee, it is our pleasure to present to you the proceedings of the Third GI SIG SIDAR Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA). DIMVA is organized by the Special Interest Group Security - Intrusion Detection and Response (SIDAR) of the German Informatics Society (GI) as an annual conference that brings together experts from throughout and outside Europe to discuss the state of the art in the areas of intrusion detection, malware detection and vulnerability assessment.

The DIMVA 2006 Program Committee received 41 submissions from 21 countries. All submissions were carefully reviewed by Program Committee members or external experts according to the criteria of scientific novelty, importance to the field and technical quality. The final selection took place at a Program Committee meeting held on March 10, 2006, in Berlin, Germany. Eleven full papers were selected for presentation and publication in the conference proceedings. In addition, two papers were selected for presentation in the best-practices track of the conference.

The conference took place on July 13-14, 2006, at the conference center of the Berlin-Brandenburg Academy of Sciences in Berlin, Germany. The program featured both theoretical and practical research results, which were grouped into six sessions. Invited talks were given by two internationally renowned security experts: John McHugh, Dalhousie University, Canada, and Michael Behringer, Cisco Systems, France. The conference program was complemented by the European Capture-the-Flag contest CIPHER (Challenges in Informatics: Programming, Hosting and Exploring), a rump session as well as the graduate workshop SPRING, which gave PhD students and young researchers an opportunity to present and discuss their current work and recent results.

We sincerely thank all those who submitted papers as well as the Program Committee members and the external reviewers for their valuable contributions.

For further details please refer to the DIMVA 2006 website at <http://www.dimva.org/dimva2006>.

July 2006

Roland Büschkes  
Pavel Laskov

# Organization

DIMVA 2006 was organized by the Special Interest Group Security - Intrusion Detection and Response (SIDAR) of the German Informatics Society (GI), in cooperation with the IEEE Task Force on Information Assurance.

## Organizing Committee

General Chair	Pavel Laskov (Fraunhofer FIRST, Germany)
Program Chair	Roland Büschkes (RWE AG, Germany)
Sponsor Chair	Marc Heuse (n.runs, Germany)

## Program Committee

Phil Attfield	Northwest Security Institute, USA
Thomas Biege	SUSE LINUX Products GmbH, Germany
Marc Dacier	Institut Eurécom, France
Hervé Debar	France Telecom R&D, France
Sven Dietrich	Carnegie Mellon University, USA
Toralv Dirro	McAfee, Germany
Ulrich Flegel	University of Dortmund, Germany
Dirk Häger	BSI, Germany
Bernhard Hämmerli	HTA Luzern, Switzerland
Oliver Heinz	arago AG, Germany
Peter Herrmann	NTNU Trondheim, Norway
Marc Heuse	n.runs, Germany
Erland Jonsson	Chalmers University of Technology, Sweden
Klaus Julisch	IBM Research, USA
Engin Kirda	Technical University Vienna, Austria
Hartmut König	BTU Cottbus, Germany
Klaus-Peter Kossakowski	DFN-Cert, Germany
Christopher Kruegel	Technical University Vienna, Austria
Jens Meggers	Symantec, USA
Michael Meier	University of Dortmund, Germany
Achim Müller	Deutsche Telekom Laboratories, Germany
Martin Naedele	ABB Corporate Research, Switzerland
Dirk Schadt	Computer Associates, Germany
Robin Sommer	ICIR/ICSI, USA
Axel Tanner	IBM Research, Switzerland
Marco Thorbrügge	ENISA, Greece
Stephen Wolthusen	Gjøvik University College, Norway

## External Reviewers

Magnus Almgren	Chalmers University of Technology, Sweden
Nenad Jovanovic	Technical University Vienna, Austria
Corrado Leita	Institut Eurécom, France
Andreas Moser	Technical University Vienna, Austria
Sebastian Schmerl	BTU Cottbus, Germany
Olivier Thonnard	Institut Eurécom, France

## Steering Committee

Chairs	Ulrich Flegel (University of Dortmund, Germany)
	Michael Meier (University of Dortmund, Germany)
Members	Roland Büschkes (RWE AG, Germany)
	Marc Heuse (n.runs, Germany)
	Klaus Julisch (IBM Research, USA)
	Christopher Kruegel (Technical University Vienna, Austria)

## Sponsoring Institutions

**McAfee®**



# Table of Contents

## Code Analysis

Using Type Qualifiers to Analyze Untrusted Integers and Detecting Security Flaws in C Programs <i>Ebrima N. Ceesay, Jingmin Zhou, Michael Gertz, Karl Levitt, Matt Bishop</i> .....	1
Using Static Program Analysis to Aid Intrusion Detection <i>Manuel Egele, Martin Szydlowski, Engin Kirda, Christopher Kruegel</i> .....	17

## Intrusion Detection

An SVM-Based Masquerade Detection Method with Online Update Using Co-occurrence Matrix <i>Liangwen Chen, Masayoshi Aritsugi</i> .....	37
Network-Level Polymorphic Shellcode Detection Using Emulation <i>Michalis Polychronakis, Kostas G. Anagnostakis, Evangelos P. Markatos</i> .....	54
Detecting Unknown Network Attacks Using Language Models <i>Konrad Rieck, Pavel Laskov</i> .....	74

## Threat Protection and Response

Using Labeling to Prevent Cross-Service Attacks Against Smart Phones <i>Collin Mulliner, Giovanni Vigna, David Dagon, Wenke Lee</i> .....	91
Using Contextual Security Policies for Threat Response <i>Hervé Debar, Yohann Thomas, Nora Boulahia-Cuppens, Frédéric Cuppens</i> .....	109

## Malware and Forensics

Detecting Self-mutating Malware Using Control-Flow Graph Matching <i>Danilo Bruschi, Lorenzo Martignoni, Mattia Monga</i> .....	129
--	-----

Digital Forensic Reconstruction and the Virtual Security Testbed ViSe  
*André Arnes, Paul Haas, Giovanni Vigna, Richard A. Kemmerer . . . .* 144

**Deployment Scenarios**

A Robust SNMP Based Infrastructure for Intrusion Detection and  
Response in Tactical MANETs  
*Marko Jahnke, Jens Tölle, Sascha Lettgen, Michael Bussmann,  
Uwe Weddige . . . . .* 164

A Fast Worm Scan Detection Tool for VPN Congestion Avoidance  
*Arno Wagner, Thomas Dübendorfer, Roman Hiestand,  
Christoph Göldi, Bernhard Plattner . . . . .* 181

**Author Index . . . . .** 195