Lecture Notes in Computer Science **10327**

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

More information about this series at http://www.springer.com/series/7410

Michalis Polychronakis · Michael Meier (Eds.)

Detection of Intrusions and Malware, and Vulnerability Assessment

14th International Conference, DIMVA 2017
Bonn, Germany, July 6–7, 2017
Proceedings

Springer

Editors
Michalis Polychronakis
Stony Brook University
Stony Brook, NY
USA

Michael Meier
University of Bonn and Fraunhofer FKIE
Bonn
Germany

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-60875-4 ISBN 978-3-319-60876-1 (eBook)
DOI 10.1007/978-3-319-60876-1

Library of Congress Control Number: 2017943061

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

On behalf of the Program Committee, it is our pleasure to present the proceedings of the 14th International Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), which took place in Bonn, Germany, during July 6–7, 2017. Since 2004, DIMVA has been bringing together leading researchers and practitioners from academia, industry, and government to present and discuss novel security research in the broader areas of intrusion detection, malware analysis, and vulnerability assessment. DIMVA is organized by the Special Interest Group – Security, Intrusion Detection, and Response (SIDAR) – of the German Informatics Society (GI).

This year, DIMVA received 67 valid submissions from academic and industrial organizations from 25 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 of papers was decided during a day-long Program Committee meeting that took place at Stony Brook University, USA, on April 7, 2017. In all, 18 full papers were selected for presentation at the conference and publication in the proceedings, resulting in an acceptance rate of 26.9%. The accepted papers present novel ideas, techniques, and applications in important areas of computer security, including enclaves and isolation, malware analysis, cyber-physical systems, detection and protection, code analysis, and Web security. Beyond the research papers, the conference program also included two insightful keynote talks by Thomas Dullien (Google) and Prof. Christopher Kruegel (University of California at Santa Barbara).

A successful conference is the result of the joint effort of many people. We would like to express our appreciation to the Program Committee members and external reviewers for the time spent reviewing papers, participating in the online discussion, attending the Program Committee meeting in Stony Brook, and shepherding some of the papers to ensure the highest quality possible. We also deeply thank the members of the Organizing Committee for their hard work in making DIMVA 2017 such a successful event, and our invited speakers for their willingness to participate in the conference. We are wholeheartedly thankful to our sponsors ERNW, genua, Google, Huawei, Rohde & Schwarz Cybersecurity, Springer, and VMRay for generously supporting DIMVA 2017. We also thank Springer for publishing these proceedings as part of their LNCS series, and the DIMVA Steering Committee for their continuous support and assistance.

Finally, DIMVA 2017 would not have been possible without the authors who submitted their work and presented their contributions as well as the attendees who came to the conference. We would like to thank them all, and we look forward to their future contributions to DIMVA.

July 2017

Michalis Polychronakis
Michael Meier

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

Michael Meier	University of Bonn and Fraunhofer FKIE, Germany

Program Chair

Michalis Polychronakis	Stony Brook University, USA

Steering Committee (Chairs)

Ulrich Flegel	Infineon Technologies, Germany
Michael Meier	University of Bonn and Fraunhofer FKIE, Germany

Steering Committee (Members)

Magnus Almgren	Chalmers University of Technology, Sweden
Herbert Bos	Vrije Universiteit Amsterdam, The Netherlands
Danilo M. Bruschi	Università degli Studi di Milano, Italy
Roland Bueschkes	RWE AG, Germany
Juan Caballero	IMDEA Software Institute, Spain
Lorenzo Cavallaro	Royal Holloway, University of London, UK
Herve Debar	Telecom SudParis, France
Sven Dietrich	City University of New York, USA
Bernhard Haemmerli	Acris GmbH and HSLU Lucerne, Switzerland
Thorsten Holz	Ruhr University Bochum, Germany
Marko Jahnke	CSIRT, German Federal Authority, Germany
Klaus Julisch	Deloitte, Switzerland
Christian Kreibich	ICSI, USA
Christopher Kruegel	University of California, Santa Barbara, USA
Pavel Laskov	Huawei European Research Center, Germany
Federico Maggi	Trend Micro, Italy
Konrad Rieck	TU Braunschweig, Germany
Robin Sommer	ICSI/LBNL, USA
Urko Zurutuza	Mondragon University, Spain

Program Committee

Magnus Almgren	Chalmers University of Technology, Sweden
Leyla Bilge	Symantec Research Labs, France

Herbert Bos	Vrije Universiteit Amsterdam, The Netherlands
Lorenzo Cavallaro	Royal Holloway, University of London, UK
Mauro Conti	University of Padua, Italy
Baris Coskun	Amazon, USA
Lucas Davi	University of Duisburg-Essen, Germany
Herve Debar	Telecom SudParis, France
Sven Dietrich	City University of New York, USA
Brendan Dolan-Gavitt	NYU, USA
Adam Doupé	Arizona State University, USA
Zakir Durumeric	University of Michigan, USA
Manuel Egele	Boston University, USA
Ulrich Flegel	Infineon Technologies AG, Germany
Cristiano Giuffrida	Vrije Universiteit Amsterdam, The Netherlands
Martin Johns	SAP Research, Germany
Alexandros Kapravelos	North Carolina State University, USA
Vasileios Kemerlis	Brown University, USA
Christian Kreibich	ICSI, USA
Christopher Kruegel	University of California, Santa Barbara, USA
Andrea Lanzi	University of Milan, Italy
Pavel Laskov	Huawei European Research Center, Germany
Corrado Leita	Lastline, UK
Zhiqiang Lin	University of Texas at Dallas, USA
Martina Lindorfer	University of California, Santa Barbara, USA
Federico Maggi	Trend Micro, Italy
Stefan Mangard	Graz University of Technology, Austria
Michael Meier	University of Bonn and Fraunhofer FKIE, Germany
Collin Mulliner	Square, USA
Nick Nikiforakis	Stony Brook University, USA
Roberto Perdisci	University of Georgia, USA
Jason Polakis	University of Illinois at Chicago, USA
Konrad Rieck	TU Braunschweig, Germany
Christian Rossow	Saarland University, Germany
Gianluca Stringhini	University College London, UK
Urko Zurutuza	Mondragon University, Spain

Additional Reviewers

Tooska Dargahi	Panagiotis Ilia	Srdan Moraca
Michalis Diamantaris	Mikel Iturbe	Raphael Otto
Patrick Duessel	Daniele Lain	Pablo Picazo-Sanchez
Hossein Fereidooni	Clémentine Maurice	Tobias Wahl
Daniel Gruss	Veelasha Moonsamy	

Contents