# Lecture Notes in Computer Science 11543

*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

Roberto Perdisci · Clémentine Maurice ·
Giorgio Giacinto · Magnus Almgren (Eds.)

# Detection of Intrusions and Malware, and Vulnerability Assessment

16th International Conference, DIMVA 2019
Gothenburg, Sweden, June 19–20, 2019
Proceedings

Springer

*Editors*
Roberto Perdisci
University of Georgia
Athens, GA, USA

Georgia Institute of Technology
Atlanta, GA, USA

Giorgio Giacinto
University of Cagliari
Cagliari, Italy

Clémentine Maurice
University of Rennes, CNRS, IRISA
Rennes, France

Magnus Almgren
Chalmers University of Technology
Gothenburg, Sweden

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-22037-2 ISBN 978-3-030-22038-9 (eBook)
https://doi.org/10.1007/978-3-030-22038-9

LNCS Sublibrary: SL4 – Security and Cryptology



This Springer imprint is published by the registered company Springer Nature Switzerland 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 16th International Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), which took place in Gothenburg, Sweden, June 19–20, 2019. 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 80 valid submissions from academic and industrial organizations from more than 40 different institutions across 16 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 the Georgia Institute of Technology in Atlanta, USA, on April 8, 2019. The Program Committee selected 23 full papers for presentation at the conference and publication in the proceedings, resulting in an acceptance rate of 28.8%. The accepted papers present novel ideas, techniques, and applications in important areas of computer security, including Web and browser security, malware analysis and defense, security of industrial systems and cyber physical systems, attack mitigation, network security, and software security. The conference program also included two insightful keynote talks by Prof. Mathias Payer (École polytechnique fédérale de Lausanne) and Prof. Frank Piessens (Katholieke Universiteit Leuven).

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 Atlanta, 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 2019 such a successful event. We are wholeheartedly thankful to our sponsors Trend Micro, Svenska kraftnät, Recorded Future, Palo Alto Networks, and Springer for generously supporting DIMVA 2019. 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 2019 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.

June 2019

Roberto Perdisci
Clémentine Maurice
Giorgio Giacinto
Magnus Almgren

# 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**

| | |
|---|---|
| Magnus Almgren | Chalmers University of Technology, Sweden |

**Program Chair**

| | |
|---|---|
| Roberto Perdisci | University of Georgia and Georgia Institute of Technology, USA |

**Program Co-chair**

| | |
|---|---|
| Clémentine Maurice | CNRS, IRISA, France |

**Publications Chair**

| | |
|---|---|
| Giorgio Giacinto | University of Cagliari, Italy |

**Publicity Chair**

| | |
|---|---|
| Kyu Hyung Lee | University of Georgia, USA |

**Sponsor Chair**

| | |
|---|---|
| Xavier Bellekens | Abertay University, UK |

**Local Arrangements Chair**

| | |
|---|---|
| Pablo Picazo-Sanchez | Chalmers University of Technology and University of Gothenburg, Sweden |

## Steering Committee (Chairs)

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

## Steering Committee

| | |
|---|---|
| Magnus Almgren | Chalmers University of Technology, Sweden |
| Sébastien Bardin | CEA, France |
| Gregory Blanc | Télécom SudParis, France |

| | |
|---|---|
| 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 |
| Hervé Debar | Télécom SudParis, France |
| Sven Dietrich | City University of New York, USA |
| Cristiano Giuffrida | Vrije Universiteit Amsterdam, The Netherlands |
| Bernhard Haemmerli | Acris GmbH and HSLU Lucerne, Switzerland |
| Thorsten Holz | Ruhr-Universität Bochum, Germany |
| Marko Jahnke | CSIRT, German Federal Authority, Germany |
| Klaus Julisch | Deloitte, Switzerland |
| Christian Kreibich | ICSI, USA |
| Christopher Kruegel | UC Santa Barbara, USA |
| Pavel Laskov | Universität Liechtenstein, Liechtenstein |
| Federico Maggi | Trend Micro Research, Italy |
| Michalis Polychronakis | Stony Brook University, USA |
| Konrad Rieck | TU Braunschweig, Germany |
| Jean-Pierre Seifert | Technical University Berlin, Germany |
| Robin Sommer | ICSI/LBNL, USA |
| Urko Zurutuza | Mondragon University, Spain |

## Program Committee

| | |
|---|---|
| Manos Antonakakis | Georgia Institute of Technology, USA |
| Marco Balduzzi | Trend Micro Research, Italy |
| Leyla Bilge | Symantec Research Labs, France, |
| Lorenzo Cavallaro | King's College London, UK |
| Gabriela Ciocarlie | SRI International, USA |
| Baris Coskun | Amazon Web Services, USA |
| Lorenzo De Carli | Worcester Polytechnic Institute, USA |
| Hervé Debar | Télécom SudParis, France |
| Sven Dietrich | City University of New York, USA |
| Brendan Dolan-Gavitt | NYU, USA |
| Adam Doupé | Arizona State University, USA |
| Manuel Egele | Boston University, USA |
| Ulrich Flegel | Infineon Technologies AG, Germany |
| Yanick Fratantonio | EURECOM, France |
| Giorgio Giacinto | University of Cagliari, Italy |
| Neil Gong | Iowa State University, USA |
| Thorsten Holz | Ruhr-Universität Bochum, Germany |
| Kyu Hyung Lee | University of Georgia, USA |
| Sotiris Ioannidis | FORTH, Greece |
| Vasileios Kemerlis | Brown University, USA |
| Katharina Krombholz | CISPA Helmholtz Center for Information Security, Germany |

| | |
|---|---|
| Andrea Lanzi | University of Milan, Italy |
| Corrado Leita | Lastline, UK |
| Zhiqiang Lin | Ohio State University, USA |
| Martina Lindorfer | TU Wien, Austria |
| Xiapu Luo | The Hong Kong Polytechnic University, HK |
| Federico Maggi | Trend Micro Research, Italy |
| Michael Meier | University of Bonn and Fraunhofer FKIE, Germany |
| Jelena Mirkovic | USC ISI, USA |
| Nick Nikiforakis | Stony Brook University, USA |
| Anita Nikolich | Illinois Institute of Technology, USA |
| Daniela Oliveira | University of Florida, USA |
| Christina Poepper | New York University Abu Dhabi, UAE |
| Georgios Portokalidis | Stevens Institute of Technology, USA |
| Christian Rossow | CISPA Helmholtz Center for Information Security, Germany |
| Deborah Shands | SRI International, USA |
| Kapil Singh | IBM T.J. Watson Research Center, USA |
| Gianluca Stringhini | Boston University, USA |
| Juan Tapiador | Universidad Carlos III, Spain |
| Heng Yin | University of California Riverside, USA |
| Stefano Zanero | Politecnico di Milano, Italy |

## Additional Reviewers

| | |
|---|---|
| Ioannis Agadakos | SRI International, USA |
| Omar Alrawi | Georgia Institute of Technology, USA |
| Davide Ariu | Pluribus One, Italy |
| Thanos Avgetidis | Georgia Institute of Technology, USA |
| Babak Amin Azad | Stony Brook University, USA |
| Ala' Darabseh | NYU Abu Dhabi, UAE |
| Erick Bauman | Ohio State University, USA |
| Battista Biggio | University of Cagliari, Italy |
| Gregory Blanc | Télécom SudParis, France |
| Marcus Botacin | Federal University of Paraná, Brazil |
| Daniel Capecci | University of Florida, USA |
| Fabrício Ceschin | Federal University of Paraná, Brazil |
| Aokun Chen | University of Florida, USA |
| Sanchuan Chen | Ohio State University, USA |
| Igino Corona | Pluribus One, Italy |
| Vasu Devan | Stony Brook University, USA |
| Sergej Epp | Palo Alto Networks, Germany |
| Matthias Fassl | CISPA Helmholtz Center for Information Security, Germany |
| Tobias Fiebig | TU Delft, The Netherlands |
| Matthias Gusenbauer | SBA Research, Austria |
| Mohit Jangid | Ohio State University, USA |

| | |
|---|---|
| Konstantinos Karakatsanis | Georgia Institute of Technology, USA |
| Kleanthis Karakolios | Georgia Institute of Technology, USA |
| Panagiotis Kintis | Georgia Institute of Technology, USA |
| Athanasios Kountouras | Georgia Institute of Technology, USA |
| Shoufu Luo | City University of New York, USA |
| Davide Maiorca | University of Cagliari, Italy |
| Najmeh Miramirkhani | Stony Brook University, USA |
| Muhammad Shujaat Mirza | NYU Abu Dhabi, UAE |
| Liang Niu | NYU Abu Dhabi, UAE |
| Jaehyun Nam | KAIST, Republic of Korea |
| Thomas Papastergiou | Georgia Institute of Technology, USA |
| Fabio Pierazzi | King's College London, UK |
| Nikolaos Sapountzis | University of Florida, USA |
| Thomas Schreck | Siemens AG, Germany |
| Jeremy Seideman | City University of New York, USA |
| Mirela Silva | University of Florida, USA |
| Ruimin Sun | University of Florida, USA |
| Dennis Tatang | Ruhr-University Bochum, Germany |
| Phani Vadrevu | University of New Orleans, USA |
| Mathy Vanhoef | NYU Abu Dhabi, UAE |
| Matthias Wübbeling | University of Bonn and Fraunhofer FKIE, Germany |
| Mengya Zhang | Ohio State University, USA |

## Sponsors


TREND
MICRO™


SVENSKA
KRAFTNÄT


Recorded
Future


paloalto
NETWORKS®


Springer

# Contents