

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen 

TU Dortmund University, Dortmund, Germany

Moti Yung 

Columbia University, New York, NY, USA

More information about this series at <https://link.springer.com/bookseries/558>

Lorenzo Cavallaro · Daniel Gruss ·
Giancarlo Pellegrino · Giorgio Giacinto (Eds.)

Detection of Intrusions and Malware, and Vulnerability Assessment


19th International Conference, DIMVA 2022
Cagliari, Italy, June 29 – July 1, 2022
Proceedings

Editors

Lorenzo Cavallaro
University College London
London, UK

Giancarlo Pellegrino
CISPA Helmholtz Center for Information
Security
Saarbrücken, Germany

Daniel Gruss
Graz University of Technology
Graz, Austria

Giorgio Giacinto 
University of Cagliari
Cagliari, Italy

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-09483-5

ISBN 978-3-031-09484-2 (eBook)

<https://doi.org/10.1007/978-3-031-09484-2>

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 2022

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

Preface

We would like to welcome you all to the proceedings of the 19th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2022). It's been almost two decades since the inception of DIMVA and it is a privilege to have witnessed over the years the high-quality research that the conference has always been able to attract.

We would like to thank the Program Committee for putting a high-quality program together; reviewing is part of what most of us call “professional service” and we know that for many, if not all of us, it is actually an opportunity to nurture the next-generation of scientists and, in a way, contribute indirectly to the advancement of our research field while building a strong, diverse, and inclusive community.

This year we received 39 valid submissions and accepted 11 papers (10 full papers and one short paper), keeping DIMVA's acceptance rate competitive at 28.2%. Given the short timeframe, we built a larger PC than prior years to ensure a more manageable load. On average, each paper received three reviews and each PC member (sometimes with the help of external reviewers) received up to three papers to review.

PC members and external reviewers engaged in online discussions, exchanging more than 200 messages. Given the ongoing COVID-19 pandemic, we opted to keep discussions online, with no physical nor virtual PC meeting as the thorough discussions (and reviews) helped us to converge on a final decision quite easily in most cases.

We would like to express our gratitude to the Program Committee members and external reviewers for the time spent reviewing papers, participating in the online discussions, and shepherding some of the papers to ensure the highest quality possible. We also deeply thank the members of the Organizing Committee and the Steering Committee for their hard work. Of course, we are wholeheartedly thankful to the German Informatics Society and the University of Cagliari for supporting and hosting an in-person (fingers crossed!) DIMVA 2022.

Our final thanks go to all participants, authors, and attendees, who are at the core of our conference and community – thank you so much for always making DIMVA and its 19th edition such an interesting conference.

We hope that science, education, and love and respect for everyone may help us to work out differences peacefully and bring us closer than ever before. Enjoy DIMVA 2022!

June 2022

Lorenzo Cavallaro
Daniel Gruss
Giancarlo Pellegrino
Giorgio Giacinto

Organization

Steering Committee Chairs

Flegel, Ulrich
Meier, Michael

Infineon Technologies, Germany
University of Bonn and Fraunhofer FKIE,
Germany

Steering Committee

Almgren, Magnus
Bardin, Sébastien
Bilge, Leyla
Blanc, Gregory
Bos, Herbert
Bruschi, Danilo M.
Bueschkes, Roland
Caballero, Juan
Cavallaro, Lorenzo
Debar, Hervé
Dietrich, Sven
Giuffrida, Cristiano
Haemmerli, Bernhard
Holz, Thorsten
Jahnke, Marko
Julisch, Klaus
Kreibich, Christian
Kruegel, Christopher
Laskov, Pavel
Maggi, Federico
Maurice, Clémentine
Neves, Nuno
Perdisci, Roberto

Polychronakis, Michalis
Rieck, Konrad
Seifert, Jean-Pierre
Sommer, Robin
Zurutuza, Urko

Chalmers University of Technology, Sweden
CEA, France
NortonLifeLock Research Group, France
Télécom SudParis, France
Vrije Universiteit Amsterdam, The Netherlands
Università degli Studi di Milano, Italy
BearingPoint, Germany
IMDEA Software Institute, Spain
University College London, UK
Télécom SudParis, France
City University of New York, USA
Vrije Universiteit Amsterdam, The Netherlands
Acris GmbH and HSLU Lucerne, Switzerland
Ruhr-University Bochum, Germany
CSIRT, Germany
Deloitte, Switzerland
ICSI, USA
University of California, Santa Barbara, USA
University of Liechtenstein, Liechtenstein
Huawei Technologies, Italy
CNRS, CRISTAL, France
University of Lisbon, Portugal
University of Georgia and Georgia Institute of
Technology, USA
Stony Brook University, USA
TU Braunschweig, Germany
TU Berlin, Germany
ICSI, USA
Mondragon University, Spain

General Chair

Giorgio Giacinto

University of Cagliari, Italy

Program Co-chairs

Lorenzo Cavallaro

University College London, UK

Daniel Gruss

TU Graz, Austria

Publication Chair

Giancarlo Pellegrino

CISPA, Germany

Program Committee

Alis, Jorge Blasco

Royal Holloway University of London, UK

Almgren, Magnus

Chalmers University of Technology, Sweden

Arp, Daniel

TU Berlin, Germany

Bardin, Sébastien

CEA List, France

Bianchi, Antonio

Purdue University, USA

Blanc, Gregory

Télécom SudParis, France

Cono D'Elia, Daniele

Sapienza University of Rome, Italy

Dacier, Marc

KAUST, Saudi Arabia

Daniel, Lesly-Ann

KU Leuven, Belgium

Dietrich, Sven

City University of New York, USA

Dolan-Gavitt, Brendan

New York University, USA

Fratantonio, Yanick

Cisco Talos, USA

Graziano, Mariano

Cisco Talos, USA

Guarnieri, Marco

IMDEA Software Institute, Spain

Hauser, Christophe

University of Southern California, USA

Kaprayelos, Alexandros

North Carolina State University, USA

Kemerlis, Vasileios

Brown University, USA

Kinder, Johannes

Bundeswehr University Munich, Germany

Kotzias, Platon

Norton Research Labs, USA

Kruegel, Christopher

University of California, Santa Barbara, USA

Lanzi, Andrea

University of Milan, Italy

Laperdrix, Pierre

CNRS, France

Lee, Wenke

Georgia Institute of Technology, USA

Leita, Corrado

VMware, USA

Lin, Zhiqiang

Ohio State University, USA

Lipp, Moritz

Amazon Web Services, USA

Maggi, Federico

Huawei Technologies, Germany

Matic, Srdjan

IMDEA Software Institute, Spain

Meier, Michael	University of Bonn and Fraunhofer FKIE, Germany
Muench, Marius	Vrije Universiteit Amsterdam, The Netherlands
Nikiforakis, Nick	Stony Brook University, USA
Nikolich, Anita	University of Illinois at Urbana-Champaign, USA
Pagani, Fabio	University of California, Santa Barbara, USA
Palit, Tapti	Purdue University, USA
Pellegrino, Giancarlo	CISPA Helmholtz Center for Information Security, Germany
Pendlebury, Feargus	Meta, USA
Pierazzi, Fabio	King's College London, UK
Razavi, Kaveh	ETH Zurich, Switzerland
Rieck, Konrad	TU Braunschweig, Germany
Schwarz, Michael	CISPA Helmholtz Center for Information Security, Germany
Sekar, R.	Stony Brook University, USA
Sgandurra, Daniele	Huawei Technologies, Germany
Shin, Seungwon	KAIST, South Korea
Stringhini, Gianluca	Boston University, USA
Suarez-Tangil, Guillermo	IMDEA Networks Institute, Spain
Tapiador, Juan	Universidad Carlos III de Madrid, Spain
Thomas, Sam L.	BINARLY, Inc., UK
Toffalini, Flavio	EPFL, Switzerland
Van Bulck, Jo	KU Leuven, Belgium
Wang, Gang	University of Illinois at Urbana-Champaign, USA
Wressnegger, Christian	Karlsruhe Institute of Technology, Germany
Yap, Roland	National University of Singapore, Singapore
Zanero, Stefano	Politecnico di Milano, Italy
Šrندیć, Nedim	Huawei Munich Research Center, Germany

Additional Reviewers

Dannehl, Moritz	Bundeswehr University Munich, Germany
Menguy, Grégoire	CEA LIST, Université Paris-Saclay, France
Recoules, Frédéric	CEA LIST, Université Paris-Saclay, France

Contents

Hybrid Pruning: Towards Precise Pointer and Taint Analysis	1
<i>Dipanjan Das, Priyanka Bose, Aravind Machiry, Sebastiano Mariani, Yan Shoshitaishvili, Giovanni Vigna, and Christopher Kruegel</i>	
Establishing the Contaminating Effect of Metadata Feature Inclusion in Machine-Learned Network Intrusion Detection Models	23
<i>Laurens D'hooge, Miel Verkerken, Bruno Volckaert, Tim Wauters, and Filip De Turck</i>	
Extended Abstract: Effective Call Graph Fingerprinting for the Analysis and Classification of Windows Malware	42
<i>Francesco Meloni, Alessandro Sanna, Davide Maiorca, and Giorgio Giacinto</i>	
COBRA-GCN: Contrastive Learning to Optimize Binary Representation Analysis with Graph Convolutional Networks	53
<i>Michael Wang, Alexander Interrante-Grant, Ryan Whelan, and Tim Leek</i>	
Prioritizing Antivirus Alerts on Internal Enterprise Machines	75
<i>Shay Sakazi, Yuval Elovici, and Asaf Shabtai</i>	
VANDALIR: Vulnerability Analyses Based on Datalog and LLVM-IR	96
<i>Joschua Schilling and Tilo Müller</i>	
Branch Different - Spectre Attacks on Apple Silicon	116
<i>Lorenz Hetterich and Michael Schwarz</i>	
MPKAlloc: Efficient Heap Meta-data Integrity Through Hardware Memory Protection Keys	136
<i>William Blair, William Robertson, and Manuel Egele</i>	
A Human in Every APE: Delineating and Evaluating the Human Analysis Systems of Anti-Phishing Entities	156
<i>Bhupendra Acharya and Phani Vadrevu</i>	
Amplification Chamber: Dissecting the Attack Infrastructure of Memcached DRDoS Attacks	178
<i>Mizuki Kondo, Rui Tanabe, Natsuo Shintani, Daisuke Makita, Katsunari Yoshioka, and Tsutomu Matsumoto</i>	

Consistency is All I Ask: Attacks and Countermeasures on the Network
Context of Distributed Honeypots 197
 *Songsong Liu, Pengbin Feng, Jiahao Cao, Xu He, Tommy Chin,
 Kun Sun, and Qi Li*

Author Index 219