Lecture Notes in Computer Science

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

Editorial Board Members

David Hutchison
Lancaster University, Lancaster, 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, Zurich, Switzerland

John C. Mitchell
Stanford University, Stanford, CA, USA

Moni Naor
Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan
Indian Institute of Technology Madras, Chennai, India

Bernhard Steffen
TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos
University of California, Los Angeles, CA, USA

Doug Tygar
University of California, Berkeley, CA, USA
More information about this series at http://www.springer.com/series/7410
Detection of Intrusions and Malware, and Vulnerability Assessment

16th International Conference, DIMVA 2019
Gothenburg, Sweden, June 19–20, 2019
Proceedings
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 Hammerli
Acris GmbH and HSLU Lucerne, Switzerland

Thorsten Holz
Ruhr-Universität Bochum, Germany

Marko Jahne
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 Fratantonio
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
Fabricio 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
Contents

Wild Wild Web

Wild Extensions: Discovering and Analyzing Unlisted Chrome Extensions... 3
   Aidan Beggs and Alexandros Kapravelos

New Kid on the Web: A Study on the Prevalence of WebAssembly
in the Wild. ................................................................. 23
   Marius Musch, Christian Wressnegger, Martin Johns, and Konrad Rieck

Morellian Analysis for Browsers: Making Web Authentication Stronger
with Canvas Fingerprinting .................................................. 43
   Pierre Laperdrix, Gildas Avoine, Benoit Baudry, and Nick Nikiforakis

On the Perils of Leaking Referrers in Online Collaboration Services...... 67
   Beliz Kaleli, Manuel Egele, and Gianluca Stringhini

Cyber-Physical Systems

Detecting, Fingerprinting and Tracking Reconnaissance Campaigns
Targeting Industrial Control Systems. ...................................... 89
   Olivier Cabana, Amr M. Youssef, Mourad Debbabi, Bernard Lebel,
   Marthe Kassouf, and Basile L. Agba

Overshadow PLC to Detect Remote Control-Logic Injection Attacks....... 109
   Hyunguk Yoo, Sushma Kalle, Jared Smith, and Irfan Ahmed

A Security Evaluation of Industrial Radio Remote Controllers .......... 133
   Federico Maggi, Marco Balduzzi, Jonathan Andersson, Philippe Lin,
   Stephen Hilt, Akira Urano, and Rainer Vosseler

Understanding the Security of Traffic Signal Infrastructure.............. 154
   Zhenyu Ning, Fengwei Zhang, and Stephen Remias

Malware

Practical Enclave Malware with Intel SGX................................ 177
   Michael Schwarz, Samuel Weiser, and Daniel Gruss

How Does Malware Use RDTSC? A Study on Operations Executed
by Malware with CPU Cycle Measurement ............................... 197
   Yoshihiro Oyama
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>On Deception-Based Protection Against Cryptographic Ransomware</td>
<td>219</td>
</tr>
<tr>
<td>Ziya Alper Genç, Gabriele Lenzini, and Daniele Sgandurra</td>
<td></td>
</tr>
<tr>
<td>PowerDrive: Accurate De-obfuscation and Analysis of PowerShell Malware</td>
<td>240</td>
</tr>
<tr>
<td>Denis Ugarte, Davide Maiorca, Fabrizio Cara, and Giorgio Giacinto</td>
<td></td>
</tr>
<tr>
<td>Software Security and Binary Analysis</td>
<td></td>
</tr>
<tr>
<td>Memory Categorization: Separating Attacker-Controlled Data</td>
<td>263</td>
</tr>
<tr>
<td>Matthias Neugschwandtner, Alessandro Sorniotti, and Anil Kurmus</td>
<td></td>
</tr>
<tr>
<td>TypeMiner: Recovering Types in Binary Programs</td>
<td>288</td>
</tr>
<tr>
<td>Alwin Maier, Hugo Gascon, Christian Wressnegger, and Konrad Rieck</td>
<td></td>
</tr>
<tr>
<td>SAFE: Self-Attentive Function Embeddings for Binary Similarity</td>
<td>309</td>
</tr>
<tr>
<td>Luca Massarelli, Giuseppe Antonio Di Luna, Fabio Petroni, Roberto Baldoni, Leonardo Querzon</td>
<td></td>
</tr>
<tr>
<td>Triggerflow: Regression Testing by Advanced Execution Path Inspection</td>
<td>330</td>
</tr>
<tr>
<td>Iaroslav Gridin, Cesar Pereida García, Nicola Tuveri, and Billy Bob Brumley</td>
<td></td>
</tr>
<tr>
<td>Network Security</td>
<td></td>
</tr>
<tr>
<td>Large-Scale Analysis of Infrastructure-Leaking DNS Servers</td>
<td>353</td>
</tr>
<tr>
<td>Dennis Tatang, Carl Schneider, and Thorsten Holz</td>
<td></td>
</tr>
<tr>
<td>Security in Plain TXT: Observing the Use of DNS TXT Records in the Wild</td>
<td>374</td>
</tr>
<tr>
<td>Adam Portier, Henry Carter, and Charles Lever</td>
<td></td>
</tr>
<tr>
<td>No Need to Marry to Change Your Name! Attacking Profinet</td>
<td>396</td>
</tr>
<tr>
<td>IO Automation Networks Using DCP</td>
<td></td>
</tr>
<tr>
<td>Stefan Mehner and Hartmut König</td>
<td></td>
</tr>
<tr>
<td>DPX: Data-Plane eXtensions for SDN Security Service Instantiation</td>
<td>415</td>
</tr>
<tr>
<td>Taejune Park, Yeonkeun Kim, Vinod Yegneswaran, Phillip Porras,</td>
<td></td>
</tr>
<tr>
<td>Zhaoyan Xu, KyoungSoo Park, and Seungwon Shin</td>
<td></td>
</tr>
<tr>
<td>Attack Mitigation</td>
<td></td>
</tr>
<tr>
<td>Practical Password Hardening Based on TLS</td>
<td>441</td>
</tr>
<tr>
<td>Constantinos Diomedous and Elias Athanasopoulos</td>
<td></td>
</tr>
</tbody>
</table>