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

It is our pleasure to welcome you to the proceedings of the 13th International Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA 2016), which took place in Donostia-San Sebastián, Spain, during July 7–8, 2016. DIMVA is an international conference advancing the state of the art in intrusion detection, malware analysis, and vulnerability assessment. It brings together members of academia, industry, and governmental institutions to discuss novel ideas as well as mature research results.

This year, DIMVA received 66 submissions, which were carefully reviewed by the Program Committee. Each submission had at least three independent reviews. In the end, 21 papers were accepted to be presented at the conference and included in this proceedings. Of these, 19 are full papers presenting mature research results and two are extended abstracts presenting new ideas in the early stages of research. Overall, the acceptance rate was 31.8%. The accepted papers present novel ideas, techniques, and applications in important areas of computer security including vulnerability detection, attack prevention, Web security, malware detection and classification, authentication, data leakage prevention, and countering evasive techniques such as obfuscation. Beyond the research papers, the program also included insightful keynote talks by Prof. Christopher Kruegel (University of California at Santa Barbara) and by David Barroso (CounterCraft).

Many individuals and organizations contributed to the success of DIMVA 2016. First of all, we would like to express our appreciation to the Program Committee members and external reviewers for the time spent reviewing, discussing papers, and attending the Program Committee meeting in Madrid. We are also deeply grateful to all members of the Organizing Committee for their tremendous work and for excelling in their respective tasks. The conference was also made possible thanks to the support of our sponsors Huawei and Inycom, and thanks to the collaboration of the Basque Business Development Agency (SPRI) and the Department of Education, Linguistic Policy and Culture of the Basque Government. We also thank Springer for publishing these proceedings in their LNCS series, and the DIMVA Steering Committee for continuing to bring together the conference.

Finally, the success of DIMVA hinges on the authors who contribute their work and on the attendees who come to the conference. We would like to thank them and we look forward to their next contribution to DIMVA.

July 2016

Juan Caballero
Urko Zurutuza
Ricardo J. Rodríguez
DIMVA was organized by the special interest group Security – Intrusion Detection and Response (SIDAR) of the German Informatics Society (GI).

**Organizing Committee**

**General Chair**
Urko Zurutuza
Mondragon University, Spain

**Program Chair**
Juan Caballero
IMDEA Software Institute, Spain

**Financial Chair**
Iñaki Hurtado
Mondragon University, Spain

**Publication Chair**
Ricardo J. Rodríguez
University of Zaragoza, Spain

**Steering Committee** (Chairs)
Ulrich Flegel
Infineon Technologies, Germany
Michael Meier
University of Bonn, 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
Lorenzo Cavallaro
Royal Holloway, University of London, UK
Herve Debar
Telecom SudParis, France
Sven Dietrich
City University of New York, USA – John Jay College of Criminal Justice, USA
Bernhard Haemmerli
Acris GmbH & HSLU Lucerne, Switzerland
Thorsten Holz
Ruhr-Universität Bochum, Germany
Marko Jahnke
Federal Office for Information Security, Germany
Klaus Julisch
Deloitte, Switzerland
Christian Kreibich
ICSI, USA
Christopher Kruegel
UC Santa Barbara, USA
Pavel Laskov
University of Tübingen, Germany
Federico Maggi
Politecnico di Milano, Italy
Konrad Rieck University of Göttingen, Germany
Robin Sommer ICSI/LBNL, USA

Program Committee

Manos Antonakakis Georgia Institute of Technology, USA
Marco Balduzzi Trend Micro Research, USA
Leyla Bilge Symantec Research Labs, France
Herbert Bos Vrije Universiteit, The Netherlands
Levente Buttyan Budapest University of Technology and Economics, Hungary
Mauro Conti University of Padua, Italy
Baris Coskun Yahoo! Labs, USA
Lucas Davi TU Darmstadt, Germany
Sven Dietrich John Jay College of Criminal Justice, City University of New York, USA
Brendan Dolan-Gavitt New York University, USA
Zakir Durumeric University of Michigan, USA
Nigel Edwards Hewlett Packard Laboratories, UK
Manuel Egele Boston University, USA
Ulrich Flegel Infineon Technologies AG, Germany
Vincenzo Gulisano Chalmers University of Technology, Sweden
Bernhard Haemmerli Acris GmbH, Switzerland
Sotiris Ioannidis FORTH, Greece
Somesh Jha University of Wisconsin-Madison, USA
Tim Kornau Google, Switzerland
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 SBA Research, Austria
Federico Maggi Politecnico di Milano, Italy
Jean-Yves Marion Lorraine University, France
Michael Meier University of Bonn and Fraunhofer FKIE, Germany
Simin Nadjm-Tehrani Linköping University, Sweden
Nick Nikiforakis Stony Brook University, USA
Roberto Perdisci University of Georgia and Georgia Tech, USA
Jason Polakis Columbia University, USA
Konrad Rieck University of Göttingen, Germany
Christian Rossow Saarland University, Germany
Stelios MIT, USA

Sidiropoulos-Douskos

Gianluca Stringhini University College London, UK
Juan Tapiador Carlos III University of Madrid, Spain
Yves Younan Cisco Systems, USA
Stefano Zanero Politecnico di Milano, Italy
Additional Reviewers

Daniel Arp  Lorenzo De Carli  Mizuhito Ogawa
Sebastien Bardin  Parvez Faruki  Raphael Otto
Guillaume Bonfante  Dario Fiore  Davide Quarta
Michele Carminati  Máté Horváth  Vaibhav Rastogi
Jean-Luc Danger  Kaitai Liang  Sanjay Rawat
Drew Davidson  Srdan Moraca  Valentin Tudor

Sponsoring Institutions (Gold)

Sponsoring Institutions (Silver)

Collaborators
Contents

Attacks

Subverting Operating System Properties Through Evolutionary DKOM Attacks .......................................................... 3
   Mariano Graziano, Lorenzo Flore, Andrea Lanzi, and Davide Balzarotti

DeepFuzz: Triggering Vulnerabilities Deeply Hidden in Binaries: (Extended Abstract) ........................................... 25
   Konstantin Böttinger and Claudia Eckert

Defenses

AutoRand: Automatic Keyword Randomization to Prevent Injection Attacks ......................................................... 37
   Jeff Perkins, Jordan Eikenberry, Alessandro Coglio, Daniel Willenson, Stelios Sidiropoulos-Douskos, and Martin Rinard

AVRAND: A Software-Based Defense Against Code Reuse Attacks for AVR Embedded Devices .......................... 58
   Sergio Pastrana, Juan Tapiador, Guillermo Suarez-Tangil, and Pedro Peris-López

Towards Vulnerability Discovery Using Staged Program Analysis ................................................................. 78
   Bhargava Shastry, Fabian Yamaguchi, Konrad Rieck, and Jean-Pierre Seifert

Malware Detection

Comprehensive Analysis and Detection of Flash-Based Malware ................................................................. 101
   Christian Wressnegger, Fabian Yamaguchi, Daniel Arp, and Konrad Rieck

Reviewer Integration and Performance Measurement for Malware Detection .................................................... 122
   Brad Miller, Alex Kantchelian, Michael Carl Tschantz, Sadia Afroz, Rekha Bachwani, Riyaz Faizullahbey, Ling Huang, Vaishaal Shankar, Tony Wu, George Yiu, Anthony D. Joseph, and J.D. Tygar

On the Lack of Consensus in Anti-Virus Decisions: Metrics and Insights on Building Ground Truths of Android Malware ......................... 142
   Médéric Hurier, Kevin Allix, Tegawendé F. Bissyandé, Jacques Klein, and Yves Le Traon
Evasion

Probfuscation: An Obfuscation Approach Using Probabilistic Control Flows .......................................................... 165
Andre Pawlowski, Moritz Contag, and Thorsten Holz

RAMBO: Run-Time Packer Analysis with Multiple Branch Observation ........ 186
Xabier Ugarte-Pedrero, Davide Balzarotti, Igor Santos, and Pablo G. Bringas

Detecting Hardware-Assisted Virtualization ........................................ 207
Michael Brengel, Michael Backes, and Christian Rossow

Web Security

Financial Lower Bounds of Online Advertising Abuse: A Four Year Case Study of the TDSS/TDL4 Botnet ......................................................... 231
Yizheng Chen, Panagiotis Kintis, Manos Antonakakis, Yacin Nadji, David Dagon, Wenke Lee, and Michael Farrell

Google Dorks: Analysis, Creation, and New Defenses .......................... 255
Flavio Toffalini, Maurizio Abbà, Damiano Carra, and Davide Balzarotti

Data Leaks

Flush+Flush: A Fast and Stealthy Cache Attack .................................. 279
Daniel Gruss, Clémentine Maurice, Klaus Wagner, and Stefan Mangard

Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript .... 300
Daniel Gruss, Clémentine Maurice, and Stefan Mangard

Detile: Fine-Grained Information Leak Detection in Script Engines ........ 322
Robert Gawlik, Philipp Koppe, Benjamin Kollenda, Andre Pawlowski, Behrad Garmany, and Thorsten Holz

Understanding the Privacy Implications of ECS: (Extended Abstract) .... 343
Panagiotis Kintis, Yacin Nadji, David Dagon, Michael Farrell, and Manos Antonakakis

Authentication

Analysing the Security of Google’s Implementation of OpenID Connect .... 357
Wanpeng Li and Chris J. Mitchell

Leveraging Sensor Fingerprinting for Mobile Device Authentication ....... 377
Thomas Hupperich, Henry Hosseini, and Thorsten Holz
Malware Classification

MtNet: A Multi-task Neural Network for Dynamic Malware Classification 399
  Wenyi Huang and Jack W. Stokes

Adaptive Semantics-Aware Malware Classification 419
  Bojan Kolosnjaji, Apostolis Zarras, Tamas Lengyel, George Webster,
  and Claudia Eckert

Author Index 441