

Contents

Attacks

Subverting Operating System Properties Through Evolutionary DKOM Attacks.	3
<i>Mariano Graziano, Lorenzo Flore, Andrea Lanzi, and Davide Balzarotti</i>	
DeepFuzz: Triggering Vulnerabilities Deeply Hidden in Binaries: (Extended Abstract).	25
<i>Konstantin Böttinger and Claudia Eckert</i>	

Defenses

AutoRand: Automatic Keyword Randomization to Prevent Injection Attacks.	37
<i>Jeff Perkins, Jordan Eikenberry, Alessandro Coglio, Daniel Willenson, Seliios Sidiroglou-Douskos, and Martin Rinard</i>	
AVRAND: A Software-Based Defense Against Code Reuse Attacks for AVR Embedded Devices	58
<i>Sergio Pastrana, Juan Tapiador, Guillermo Suarez-Tangil, and Pedro Peris-López</i>	
Towards Vulnerability Discovery Using Staged Program Analysis.	78
<i>Bhargava Shastry, Fabian Yamaguchi, Konrad Rieck, and Jean-Pierre Seifert</i>	

Malware Detection

Comprehensive Analysis and Detection of Flash-Based Malware.	101
<i>Christian Wressnegger, Fabian Yamaguchi, Daniel Arp, and Konrad Rieck</i>	
Reviewer Integration and Performance Measurement for Malware Detection.	122
<i>Brad Miller, Alex Kantchelian, Michael Carl Tschantz, Sadia Afroz, Rekha Bachwani, Riyaz Faizullabhoj, Ling Huang, Vaishaal Shankar, Tony Wu, George Yiu, Anthony D. Joseph, and J.D. Tygar</i>	
On the Lack of Consensus in Anti-Virus Decisions: Metrics and Insights on Building Ground Truths of Android Malware.	142
<i>Médéric Hurier, Kevin Allix, Tegawendé F. Bissyandé, Jacques Klein, and Yves Le Traon</i>	

Evasion

Profuscation: 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 Nadj, 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 Nadj, 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



<http://www.springer.com/978-3-319-40666-4>

Detection of Intrusions and Malware, and Vulnerability
Assessment

13th International Conference, DIMVA 2016, San
Sebastián, Spain, July 7-8, 2016, Proceedings
Caballero, J.; Zurutuza, U.; Rodríguez, R.J. (Eds.)
2016, XIV, 442 p. 103 illus., Softcover
ISBN: 978-3-319-40666-4