

# Contents

## Enclaves and Isolation

Malware Guard Extension: Using SGX to Conceal Cache Attacks. . . . .	3
<i>Michael Schwarz, Samuel Weiser, Daniel Gruss, Clémentine Maurice, and Stefan Mangard</i>	
On the Trade-Offs in Oblivious Execution Techniques. . . . .	25
<i>Shruti Tople and Prateek Saxena</i>	
MemPatrol: Reliable Sideline Integrity Monitoring for High-Performance Systems . . . . .	48
<i>Myoung Jin Nam, Wonhong Nam, Jin-Young Choi, and Periklis Akravidis</i>	

## Malware Analysis

Measuring and Defeating Anti-Instrumentation-Equipped Malware . . . . .	73
<i>Mario Polino, Andrea Continella, Sebastiano Mariani, Stefano D'Alessio, Lorenzo Fontana, Fabio Gritti, and Stefano Zanero</i>	
DynODet: Detecting Dynamic Obfuscation in Malware . . . . .	97
<i>Danny Kim, Amir Majlesi-Kupaei, Julien Roy, Kapil Anand, Khaled ElWazeer, Daniel Buettner, and Rajeev Barua</i>	
Finding the Needle: A Study of the PE32 Rich Header and Respective Malware Triage . . . . .	119
<i>George D. Webster, Bojan Kolosnjaji, Christian von Pentz, Julian Kirsch, Zachary D. Hanif, Apostolis Zarras, and Claudia Eckert</i>	

## Cyber-physical Systems

Last Line of Defense: A Novel IDS Approach Against Advanced Threats in Industrial Control Systems . . . . .	141
<i>Mark Luchs and Christian Doerr</i>	
LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED . . . . .	161
<i>Mordechai Guri, Boris Zadov, and Yuval Elovici</i>	

A Stealth, Selective, Link-Layer Denial-of-Service Attack Against Automotive Networks . . . . .	185
<i>Andrea Palanca, Eric Evenchick, Federico Maggi, and Stefano Zanero</i>	

**Detection and Protection**

Quincy: Detecting Host-Based Code Injection Attacks in Memory Dumps . . .	209
<i>Thomas Barabosch, Niklas Bergmann, Adrian Dombeck, and Elmar Padilla</i>	
SPEAKER: Split-Phase Execution of Application Containers . . . . .	230
<i>Lingguang Lei, Jianhua Sun, Kun Sun, Chris Shenefiel, Rui Ma, Yuewu Wang, and Qi Li</i>	
Deep Ground Truth Analysis of Current Android Malware. . . . .	252
<i>Fengguo Wei, Yuping Li, Sankardas Roy, Xinming Ou, and Wu Zhou</i>	

**Code Analysis**

HumIDIFY: A Tool for Hidden Functionality Detection in Firmware . . . . .	279
<i>Sam L. Thomas, Flavio D. Garcia, and Tom Chothia</i>	
BinShape: Scalable and Robust Binary Library Function Identification Using Function Shape . . . . .	301
<i>Paria Shirani, Lingyu Wang, and Mourad Debbabi</i>	
SCVD: A New Semantics-Based Approach for Cloned Vulnerable Code Detection. . . . .	325
<i>Deqing Zou, Hanchao Qi, Zhen Li, Song Wu, Hai Jin, Guozhong Sun, Sujuan Wang, and Yuyi Zhong</i>	

**Web Security**

On the Privacy Impacts of Publicly Leaked Password Databases. . . . .	347
<i>Olivier Heen and Christoph Neumann</i>	
Unsupervised Detection of APT C&C Channels using Web Request Graphs . . . . .	366
<i>Pavlos Lamprakis, Ruggiero Dargenio, David Gugelmann, Vincent Lenders, Markus Happe, and Laurent Vanbever</i>	
Measuring Network Reputation in the Ad-Bidding Process. . . . .	388
<i>Yizheng Chen, Yacin Nadji, Rosa Romero-Gómez, Manos Antonakakis, and David Dagon</i>	

<b>Author Index</b> . . . . .	411
-------------------------------	-----

Detection of Intrusions and Malware, and Vulnerability  
Assessment

14th International Conference, DIMVA 2017, Bonn,  
Germany, July 6-7, 2017, Proceedings

Polychronakis, M.; Meier, M. (Eds.)

2017, X, 412 p. 114 illus., Softcover

ISBN: 978-3-319-60875-4