## Contents

### Enclaves and Isolation

- **Malware Guard Extension: Using SGX to Conceal Cache Attacks.**
  
  *Michael Schwarz, Samuel Weiser, Daniel Gruss, Clémentine Maurice, and Stefan Mangard*
  
  Page 3

- **On the Trade-Offs in Oblivious Execution Techniques.**
  
  *Shruti Tople and Prateek Saxena*
  
  Page 25

- **MemPatrol: Reliable Sideline Integrity Monitoring for High-Performance Systems.**
  
  *Myoung Jin Nam, Wonhong Nam, Jin-Young Choi, and Periklis Akritidis*
  
  Page 48

### Malware Analysis

- **Measuring and Defeating Anti-Instrumentation-Equipped Malware.**
  
  *Mario Polino, Andrea Continella, Sebastiano Mariani, Stefano D’Alessio, Lorenzo Fontana, Fabio Gritti, and Stefano Zanero*
  
  Page 73

- **DynODet: Detecting Dynamic Obfuscation in Malware.**
  
  *Danny Kim, Amir Majlesi-Kupaei, Julien Roy, Kapil Anand, Khaled ElWazeer, Daniel Buettner, and Rajeev Barua*
  
  Page 97

- **Finding the Needle: A Study of the PE32 Rich Header and Respective Malware Triage.**
  
  *George D. Webster, Bojan Kolosnjaji, Christian von Pentz, Julian Kirsch, Zachary D. Hanif, Apostolis Zarras, and Claudia Eckert*
  
  Page 119

### Cyber-physical Systems

- **Last Line of Defense: A Novel IDS Approach Against Advanced Threats in Industrial Control Systems.**
  
  *Mark Luchs and Christian Doerr*
  
  Page 141

- **LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED.**
  
  *Mordechai Guri, Boris Zadov, and Yuval Elovici*
  
  Page 161
A Stealth, Selective, Link-Layer Denial-of-Service Attack Against Automotive Networks ................................................. 185
   Andrea Palanca, Eric Evenchick, Federico Maggi, and Stefano Zanero

Detection and Protection

Quincy: Detecting Host-Based Code Injection Attacks in Memory Dumps . . . 209
   Thomas Barabosch, Niklas Bergmann, Adrian Dombeck, and Elmar Padilla

SPEAKER: Split-Phase Execution of Application Containers ............... 230
   Lingguang Lei, Jianhua Sun, Kun Sun, Chris Shenefiel, Rui Ma, Yuewu Wang, and Qi Li

Deep Ground Truth Analysis of Current Android Malware................. 252
   Fengguo Wei, Yuping Li, Sankardas Roy, Xinming Ou, and Wu Zhou

Code Analysis

HumIDIFy: A Tool for Hidden Functionality Detection in Firmware ........ 279
   Sam L. Thomas, Flavio D. Garcia, and Tom Chothia

BinShape: Scalable and Robust Binary Library Function Identification Using Function Shape ............................................ 301
   Paria Shirani, Lingyu Wang, and Mourad Debbabi

SCVD: A New Semantics-Based Approach for Cloned Vulnerable Code Detection .............................................................. 325
   Deqing Zou, Hanchao Qi, Zhen Li, Song Wu, Hai Jin, Guozhong Sun, Sujuan Wang, and Yuyi Zhong

Web Security

On the Privacy Impacts of Publicly Leaked Password Databases .......... 347
   Olivier Heen and Christoph Neumann

Unsupervised Detection of APT C&C Channels using Web Request Graphs 366
   Pavlos Lamprakis, Ruggiero Dargenio, David Gugelmann, Vincent Lenders, Markus Happe, and Laurent Vanbever

Measuring Network Reputation in the Ad-Bidding Process ............... 388
   Yizheng Chen, Yacin Nadji, Rosa Romero-Gómez, Manos Antonakakis, and David Dagon

Author Index ................................................................. 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