

Contents

Hardware

Ensemble Learning for Low-Level Hardware-Supported Malware Detection	3
<i>Khaled N. Khasawneh, Meltem Ozsoy, Caleb Donovick, Nael Abu-Ghazaleh, and Dmitry Ponomarev</i>	
Physical-Layer Detection of Hardware Keyloggers	26
<i>Ryan M. Gerdes and Saptarshi Mallick</i>	
Reverse Engineering Intel Last-Level Cache Complex Addressing Using Performance Counters	48
<i>Clémentine Maurice, Nicolas Le Scouarnec, Christoph Neumann, Olivier Heen, and Aurélien Francillon</i>	
Hardware-Assisted Fine-Grained Code-Reuse Attack Detection	66
<i>Pinghai Yuan, Qingkai Zeng, and Xuhua Ding</i>	

Networks

Haetae: Scaling the Performance of Network Intrusion Detection with Many-Core Processors	89
<i>Jaehyun Nam, Muhammad Jamshed, Byungkwon Choi, Dongsu Han, and KyoungSoo Park</i>	
Demystifying the IP Blackspace	111
<i>Quentin Jacquemart, Pierre-Antoine Vervier, Guillaume Urvoy-Keller, and Ernst Biersack</i>	
Providing Dynamic Control to Passive Network Security Monitoring.	133
<i>Johanna Amann and Robin Sommer</i>	

Hardening

Probabilistic Inference on Integrity for Access Behavior Based Malware Detection	155
<i>Weixuan Mao, Zhongmin Cai, Don Towsley, and Xiaohong Guan</i>	
Counteracting Data-Only Malware with Code Pointer Examination	177
<i>Thomas Kittel, Sebastian Vogl, Julian Kirsch, and Claudia Eckert</i>	
Xede: Practical Exploit Early Detection	198
<i>Meining Nie, Purui Su, Qi Li, Zhi Wang, Lingyun Ying, Jinlong Hu, and Dengguo Feng</i>	

Attack Detection I

Preventing Exploits in Microsoft Office Documents Through Content Randomization	225
<i>Charles Smutz and Angelos Stavrou</i>	
Improving Accuracy of Static Integer Overflow Detection in Binary	247
<i>Yang Zhang, Xiaoshan Sun, Yi Deng, Liang Cheng, Shuke Zeng, Yu Fu, and Dengguo Feng</i>	
A Formal Framework for Program Anomaly Detection	270
<i>Xiaokui Shu, Danfeng (Daphne) Yao, and Barbara G. Ryder</i>	

Web and Net

jÄk: Using Dynamic Analysis to Crawl and Test Modern Web Applications	295
<i>Giancarlo Pellegrino, Constantin Tschürtz, Eric Bodden, and Christian Rossow</i>	
WYSISNWIV: What You Scan Is Not What I Visit	317
<i>Qilang Yang, Dimitrios Damopoulos, and Georgios Portokalidis</i>	
SDN Rootkits: Subverting Network Operating Systems of Software-Defined Networks	339
<i>Christian Röpke and Thorsten Holz</i>	

Android

AppSpear: Bytecode Decrypting and DEX Reassembling for Packed Android Malware	359
<i>Wenbo Yang, Yuanyuan Zhang, Juanru Li, Junliang Shu, Bodong Li, Wenjun Hu, and Dawu Gu</i>	
HELDROID: Dissecting and Detecting Mobile Ransomware	382
<i>Nicoló Andronio, Stefano Zanero, and Federico Maggi</i>	
Continuous Authentication on Mobile Devices Using Power Consumption, Touch Gestures and Physical Movement of Users	405
<i>Rahul Murmuria, Angelos Stavrou, Daniel Barbará, and Dan Fleck</i>	

Privacy

Privacy Risk Assessment on Online Photos	427
<i>Haitao Xu, Haining Wang, and Angelos Stavrou</i>	

Privacy is Not an Option: Attacking the IPv6 Privacy Extension	448
<i>Johanna Ullrich and Edgar Weippl</i>	

Evaluating Solutions

Evaluation of Intrusion Detection Systems in Virtualized Environments Using Attack Injection	471
<i>Aleksandar Milenkoski, Bryan D. Payne, Nuno Antunes, Marco Vieira, Samuel Kounev, Alberto Avritzer, and Matthias Luft</i>	
Security Analysis of PHP Bytecode Protection Mechanisms	493
<i>Dario Wei�er, Johannes Dahse, and Thorsten Holz</i>	
Radmin: Early Detection of Application-Level Resource Exhaustion and Starvation Attacks	515
<i>Mohamed Elsabagh, Daniel Barbar�, Dan Fleck, and Angelos Stavrou</i>	
Towards Automatic Inference of Kernel Object Semantics from Binary Code	538
<i>Junyuan Zeng and Zhiqiang Lin</i>	

Attack Detection II

BOTWATCHER: Transparent and Generic Botnet Tracking	565
<i>Thomas Barabosch, Adrian Dombeck, Khaled Yakdan, and Elmar Gerhards-Padilla</i>	
Elite: Automatic Orchestration of Elastic Detection Services to Secure Cloud Hosting	588
<i>Yangyi Chen, Vincent Bindshaedler, XiaoFeng Wang, Stefan Berger, and Dimitrios Pendarakis</i>	
AmpPot: Monitoring and Defending Against Amplification DDoS Attacks . . .	615
<i>Lukas Kr�mer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, and Christian Rossow</i>	
Author Index	637

Research in Attacks, Intrusions, and Defenses
18th International Symposium, RAID 2015, Kyoto,
Japan, November 2-4, 2015. Proceedings
Bos, H.; Monroe, F.; Blanc, G. (Eds.)
2015, XIII, 638 p. 147 illus. in color., Softcover
ISBN: 978-3-319-26361-8