

Angelos Stavrou Herbert Bos  
Georgios Portokalidis (Eds.)

# Research in Attacks, Intrusions, and Defenses

17th International Symposium, RAID 2014  
Gothenburg, Sweden, September 17-19, 2014  
Proceedings



Springer

# Table of Contents

## Malware and Defenses

Paint It Black: Evaluating the Effectiveness of Malware Blacklists . . . . .	1
<i>Marc Kührer, Christian Rossow, and Thorsten Holz</i>	
GOLDENEYE: Efficiently and Effectively Unveiling Malware’s Targeted Environment . . . . .	22
<i>Zhaoyan Xu, Jialong Zhang, Guofei Gu, and Zhiqiang Lin</i>	
PillarBox: Combating Next-Generation Malware with Fast Forward-Secure Logging . . . . .	46
<i>Kevin D. Bowers, Catherine Hart, Ari Juels, and Nikos Triandopoulos</i>	

## Malware and Binary Analysis

Dynamic Reconstruction of Relocation Information for Stripped Binaries . . . . .	68
<i>Vasilis Pappas, Michalis Polychronakis, and Angelos D. Keromytis</i>	
Evaluating the Effectiveness of Current Anti-ROP Defenses . . . . .	88
<i>Felix Schuster, Thomas Tendyck, Jannik Pewny, Andreas Maaß, Martin Steegmanns, Moritz Contag, and Thorsten Holz</i>	
Unsupervised Anomaly-Based Malware Detection Using Hardware Features . . . . .	109
<i>Adrian Tang, Simha Sethumadhavan, and Salvatore J. Stolfo</i>	

## Web

Eyes of a Human, Eyes of a Program: Leveraging Different Views of the Web for Analysis and Detection . . . . .	130
<i>Jacopo Corbetta, Luca Invernizzi, Christopher Kruegel, and Giovanni Vigna</i>	
You Can’t Be Me: Enabling Trusted Paths and User Sub-origins in Web Browsers . . . . .	150
<i>Enrico Budianto, Yaoqi Jia, Xinshu Dong, Prateek Saxena, and Zhenkai Liang</i>	
Measuring Drive-by Download Defense in Depth . . . . .	172
<i>Nathaniel Boggs, Senyao Du, and Salvatore J. Stolfo</i>	

**Web II**

A Lightweight Formal Approach for Analyzing Security of Web Protocols . . . . .	192
<i>Apurva Kumar</i>	
Why Is CSP Failing? Trends and Challenges in CSP Adoption . . . . .	212
<i>Michael Weissbacher, Tobias Lawinger, and William Robertson</i>	
Synthetic Data Generation and Defense in Depth Measurement of Web Applications . . . . .	234
<i>Nathaniel Boggs, Hang Zhao, Senyao Du, and Salvatore J. Stolfo</i>	

**Authentication and Privacy**

A Comparative Evaluation of Implicit Authentication Schemes . . . . .	255
<i>Hassan Khan, Aaron Atwater, and Urs Hengartner</i>	
Protecting Web-Based Single Sign-on Protocols against Relying Party Impersonation Attacks through a Dedicated Bi-directional Authenticated Secure Channel . . . . .	276
<i>Yinzhi Cao, Yan Shoshitaishvili, Kevin Borgolte, Christopher Kruegel, Giovanni Vigna, and Yan Chen</i>	
Wait a Minute! A fast, Cross-VM Attack on AES . . . . .	299
<i>Gorka Irazoqui, Mehmet Sinan Inci, Thomas Eisenbarth, and Berk Sunar</i>	

**Network Security**

Count Me In: Viable Distributed Summary Statistics for Securing High-Speed Networks . . . . .	320
<i>Johanna Amann, Seth Hall, and Robin Sommer</i>	
Formal Analysis of Security Procedures in LTE - A Feasibility Study . . .	341
<i>Noomene Ben Henda and Karl Norrman</i>	
Run Away If You Can: Persistent Jamming Attacks against Channel Hopping Wi-Fi Devices in Dense Networks . . . . .	362
<i>Il-Gu Lee, Hyunwoo Choi, Yongdae Kim, Seungwon Shin, and Myungchul Kim</i>	

**Intrusion Detection and Vulnerability Analysis**

On Emulation-Based Network Intrusion Detection Systems . . . . .	384
<i>Ali Abbasi, Jos Wetzels, Wouter Bokslag, Emmanuele Zambon, and Sandro Etalle</i>	

Quantitative Evaluation of Dynamic Platform Techniques as a Defensive Mechanism .....	405
<i>Hamed Okhravi, James Riordan, and Kevin Carter</i>	
Some Vulnerabilities Are Different Than Others: Studying Vulnerabilities and Attack Surfaces in the Wild .....	426
<i>Kartik Nayak, Daniel Marino, Petros Efstathopoulos, and Tudor Dumitras</i>	
Towards a Masquerade Detection System Based on User's Tasks .....	447
<i>J. Benito Camiña, Jorge Rodríguez, and Raúl Monroy</i>	
<b>Poster Abstracts</b>	
Poster Abstract: Forensically Extracting Encrypted Contents from Stego-Files Using NTFS Artefacts .....	466
<i>Niall McGrath</i>	
Poster Abstract: Economic Denial of Sustainability (EDoS) Attack in the Cloud Using Web-Bugs .....	469
<i>Armin Slopek and Natalija Vlajic</i>	
Poster Abstract: CITRIN: Extracting Adversaries Strategies Hidden in a Large-Scale Event Log .....	473
<i>Satomi Honda, Yuki Unno, Koji Maruhashi, Masahiko Takenaka, and Satoru Torii</i>	
Poster Abstract: On Security Monitoring of Mobile Networks – Future Threats and Leveraging of Network Information .....	475
<i>Michael Liljenstam, Prajwol Kumar Nakarmi, Oscar Ohlsson, and John Mattsson</i>	
Poster Abstract: Data Leakage Detection Algorithm Based on Sequences of Activities .....	477
<i>César Guevara, Matilde Santos, and Victoria López</i>	
Poster Abstract: BPIDS - Using Business Model Specification in Intrusion Detection .....	479
<i>João Lima, Nelson Escravana, and Carlos Ribeiro</i>	
Poster Abstract: Highlighting Easily How Malicious Applications Corrupt Android Devices .....	481
<i>Radoniaina Andriatsimandefitra and Valérie Viet Triem Tong</i>	
Poster Abstract: Improving Intrusion Detection on SSL/TLS Channels by Classifying Certificates .....	483
<i>Zigang Cao, Gang Xiong, Zhen Li, and Li Guo</i>	

XIV Table of Contents

Poster Abstract: Using Financial Synthetic Data Sets for Fraud  
Detection Research ..... 485  
*Edgar Alonso Lopez-Rojas and Stefan Axelsson*

Poster Abstract: Automatic Discovery for Common Application  
Protocol Mimicry ..... 487  
*Quan Bai, Gang Xiong, Yong Zhao, and Zhenzhen Li*

**Author Index** ..... 489