

Marc Dacier · Michael Bailey
Michalis Polychronakis · Manos Antonakakis (Eds.)

Research in Attacks, Intrusions, and Defenses

20th International Symposium, RAID 2017
Atlanta, GA, USA, September 18–20, 2017
Proceedings

Contents

Software Security

- VDF: Targeted Evolutionary Fuzz Testing of Virtual Devices. 3
Andrew Henderson, Heng Yin, Guang Jin, Hao Han, and Hongmei Deng
- Static Program Analysis as a Fuzzing Aid 26
*Bhargava Shastry, Markus Leutner, Tobias Fiebig,
Kashyap Thimmaraju, Fabian Yamaguchi, Konrad Rieck,
Stefan Schmid, Jean-Pierre Seifert, and Anja Feldmann*
- Breaking Fitness Records Without Moving: Reverse Engineering
and Spoofing Fitbit 48
*Hossein Fereidooni, Jiska Classen, Tom Spink, Paul Patras,
Markus Miettinen, Ahmad-Reza Sadeghi, Matthias Hollick,
and Mauro Conti*

Intrusion Detection

- Lens on the Endpoint: Hunting for Malicious Software
Through Endpoint Data Analysis 73
*Ahmet Salih Buyukkayhan, Alina Oprea, Zhou Li,
and William Robertson*
- Redemption: Real-Time Protection Against Ransomware at End-Hosts 98
Amin Kharraz and Engin Kirda
- ILAB: An Interactive Labelling Strategy for Intrusion Detection 120
Anaël Beaunon, Pierre Chifflier, and Francis Bach

Android Security

- Precisely and Scalably Vetting JavaScript Bridge in Android Hybrid Apps. . . 143
Guangliang Yang, Abner Mendoza, Jialong Zhang, and Guofei Gu
- Filtering for Malice Through the Data Ocean: Large-Scale PHA Install
Detection at the Communication Service Provider Level 167
*Kai Chen, Tongxin Li, Bin Ma, Peng Wang, XiaoFeng Wang,
and Peiyuan Zong*
- Android Malware Clustering Through Malicious Payload Mining 192
Yuping Li, Jiyong Jang, Xin Hu, and Xinming Ou

Systems Security

- Stealth Loader: Trace-Free Program Loading for API Obfuscation. 217
*Yuhei Kawakoya, Eitaro Shioji, Yuto Otsuki, Makoto Iwamura,
 and Takeshi Yada*
- LAZARUS: Practical Side-Channel Resilient Kernel-Space Randomization. . . 238
*David Gens, Orlando Arias, Dean Sullivan, Christopher Liebchen,
 Yier Jin, and Ahmad-Reza Sadeghi*
- CFI CaRE: Hardware-Supported Call and Return Enforcement
 for Commercial Microcontrollers. 259
Thomas Nyman, Jan-Erik Ekberg, Lucas Davi, and N. Asokan

Cybercrime

- Mining on Someone Else's Dime: Mitigating Covert Mining Operations
 in Clouds and Enterprises. 287
*Rashid Tahir, Muhammad Huzaiifa, Anupam Das, Mohammad Ahmad,
 Carl Gunter, Fareed Zaffar, Matthew Caesar, and Nikita Borisov*
- BEADS: Automated Attack Discovery in OpenFlow-Based SDN Systems . . . 311
*Samuel Jero, Xiangyu Bu, Cristina Nita-Rotaru, Hamed Okhravi,
 Richard Skowyra, and Sonia Fahmy*
- Trapped by the UI: The Android Case. 334
Efthimios Alepis and Constantinos Patsakis

Cloud Security

- SGX-LAPD: Thwarting Controlled Side Channel Attacks
 via Enclave Verifiable Page Faults 357
Yangchun Fu, Erick Bauman, Raul Quinonez, and Zhiqiang Lin
- Secure In-Cache Execution. 381
Yue Chen, Mustakimur Khandaker, and Zhi Wang
- Scotch: Combining Software Guard Extensions and System Management
 Mode to Monitor Cloud Resource Usage 403
Kevin Leach, Fengwei Zhang, and Westley Weimer

Network Security

- Linking Amplification DDoS Attacks to Booter Services 427
*Johannes Krupp, Mohammad Karami, Christian Rossow,
 Damon McCoy, and Michael Backes*

Practical and Accurate Runtime Application Protection Against DoS Attacks	450
<i>Mohamed Elsabagh, Dan Fleck, Angelos Stavrou, Michael Kaplan, and Thomas Bowen</i>	
Exploring the Ecosystem of Malicious Domain Registrations in the .eu TLD	472
<i>Thomas Vissers, Jan Spooren, Pieter Agten, Dirk Jumpertz, Peter Janssen, Marc Van Wesemael, Frank Piessens, Wouter Joosen, and Lieven Desmet</i>	
Author Index	495