

1. Record Nr.	UNISA996465562803316
Titolo	Research in Attacks, Intrusions, and Defenses [[electronic resource]] : 20th International Symposium, RAID 2017, Atlanta, GA, USA, September 18–20, 2017, Proceedings / / edited by Marc Dacier, Michael Bailey, Michalis Polychronakis, Manos Antonakakis
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
ISBN	3-319-66332-1
Edizione	[1st ed. 2017.]
Descrizione fisica	1 online resource (XIII, 496 p. 115 illus.)
Collana	Security and Cryptology ; ; 10453
Disciplina	004
Soggetti	Computer security Data protection Data encryption (Computer science) Management information systems Computer science Computer communication systems Operating systems (Computers) Systems and Data Security Security Cryptology Management of Computing and Information Systems Computer Communication Networks Operating Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	VDF: Targeted Evolutionary Fuzz Testing of Virtual Devices -- Static Program Analysis as a Fuzzing Aid -- Breaking Fitness Records without Moving: Reverse Engineering and Spoofing Fitbit -- Lens on the endpoint: Hunting for malicious software through endpoint data analysis -- Redemption: Real-time Protection Against Ransomware at End-Hosts -- ILAB: An Interactive Labelling Strategy for Intrusion Detection -- Precisely and Scalably Vetting JavaScript Bridge In Android

Hybrid Apps -- Filtering for Malice through the Data Ocean: Large-Scale PHA Install Detection at the Communication Service Provider Level
-- Android Malware Clustering through Malicious Payload Mining --
Stealth Loader: Trace-free Program Loading for API Obfuscation --
LAZARUS: Practical Side-channel Resilient Kernel-Space Randomization
-- CFI CaRE: Hardware-supported Call and Return Enforcement for Commercial Microcontrollers -- Mining on Someone Else's
Dime: Mitigating Covert Mining Operations in Clouds and Enterprises
-- BEADS: Automated Attack Discovery in OpenFlow-based SDN Systems -- Trapped by the UI: The Android case -- Thwarting Controlled Side Channel Attacks via Enclave Verifiable Page Faults --
Secure In-Cache Execution -- Scotch: Combining Software Guard Extensions and System Management Mode to Monitor Cloud Resource Usage -- Linking Amplification DDoS Attacks to Booter Services --
Practical and Accurate Runtime Application Protection against DoS Attacks -- Exploring the ecosystem of malicious domain registrations in the .eu TLD.

Sommario/riassunto

This book constitutes the refereed conference proceedings of the 20th International Symposium on Research in Attacks, Intrusions, and Defenses, RAID 2017, held in Atlanta, GA, USA, in September 2017. The 21 revised full papers were selected from 105 submissions. They are organized in the following topics: software security, intrusion detection, systems security, android security, cybercrime, cloud security, network security.
