1. Record Nr. UNINA9910151858103321

Autore	Zhang Mu
Titolo	Android Application Security : A Semantics and Context-Aware Approach / / by Mu Zhang, Heng Yin
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2016
ISBN	3-319-47812-5
Edizione	[1st ed. 2016.]
Descrizione fisica	1 online resource (XI, 105 p. 37 illus., 29 illus. in color.)
Collana	SpringerBriefs in Computer Science, , 2191-5768
Disciplina	005.365
Soggetti	Computer security Computer networks Electrical engineering Systems and Data Security Computer Communication Networks Communications Engineering, Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references at the end of each chapters.
Nota di contenuto	Introduction -- Background -- Semantics-Aware Android Malware Classification -- Automatic Generation of Vulnerability-Specific Patches for Preventing Component Hijacking Attacks -- Efficient and Context-Aware Privacy Leakage Confinement -- Automatic Generation of Security-Centric Descriptions for Android Apps -- Limitation and Future Work -- Conclusion.
Sommario/riassunto	This SpringerBrief explains the emerging cyber threats that undermine Android application security. It further explores the opportunity to leverage the cutting-edge semantics and context–aware techniques to defend against such threats, including zero-day Android malware, deep software vulnerabilities, privacy breach and insufficient security warnings in app descriptions. The authors begin by introducing the background of the field, explaining the general operating system, programming features, and security mechanisms. The authors capture the semantic-level behavior of mobile applications and use it to reliably detect malware variants and zero-day malware. Next, they propose an automatic patch generation technique to detect and block dangerous

information flow. A bytecode rewriting technique is used to confine privacy leakage. User-awareness, a key factor of security risks, is addressed by automatically translating security-related program semantics into natural language descriptions. Frequent behavior mining is used to discover and compress common semantics. As a result, the produced descriptions are security-sensitive, human-understandable and concise. By covering the background, current threats, and future work in this field, the brief is suitable for both professionals in industry and advanced-level students working in mobile security and applications. It is valuable for researchers, as well.