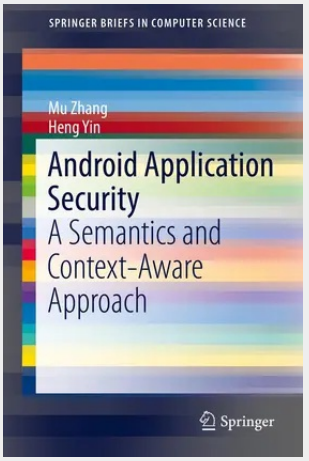
Zhang / Yin

Android Application Security

A Semantics and Context-Aware Approach



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 languagedescriptions. 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.

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 languagedescriptions. 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.

53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783319478111
Medium: Buch
ISBN: 978-3-319-47811-1
Verlag: Springer
Erscheinungstermin: 24.11.2016
Sprache(n): Englisch
Auflage: 1. Auflage 2016
Serie: SpringerBriefs in Computer Science
Produktform: Kartoniert
Gewicht: 1942 g
Seiten: 105
Format (B x H): 155 x 235 mm

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)