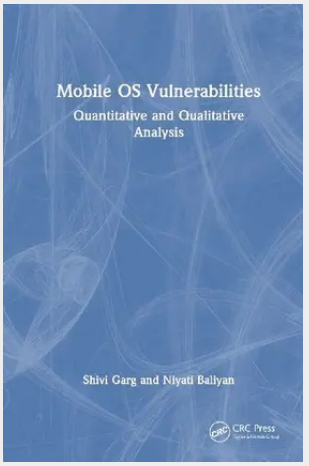
Garg / Baliyan

Mobile OS Vulnerabilities

Quantitative and Qualitative Analysis



This is book offers in-depth analysis of security vulnerabilities in different mobile operating systems. It provides methodology and solutions for handling Android malware and vulnerabilities and transfers the latest knowledge in machine learning and deep learning models towards this end. Further, it presents a comprehensive analysis of software vulnerabilities based on different technical parameters such as causes, severity, techniques, and software systems' type. Moreover, the book also presents the current state of the art in the domain of software threats and vulnerabilities. This would help analyze various threats that a system could face, and subsequently, it could guide the securityengineer to take proactive and cost-effective countermeasures. Security threats are escalating exponentially, thus posing a serious challenge to mobile platforms. Android and iOS are prominent due to their enhanced capabilities and popularity among users. Therefore, it is important to compare these two mobile platforms based on security aspects. Android proved to be more vulnerable compared to iOS. The malicious apps can cause severe repercussions such as privacy leaks, app crashes, financial losses (caused by malware triggered premium rate SMSs), arbitrary code installation, etc. Hence, Android security is a major concern amongst researchers as seen in the last few years. This book provides an exhaustive review of all the existing approaches in a structured format. The book also focuses on the detection of malicious applications that compromise users' security and privacy, the detection performance of the different program analysis approach, and the influence of different input generators during static and dynamic analysis on detection performance. This book presents a novel method using an ensemble classifier scheme for detecting malicious applications, which is less susceptible to the evolution of the Android ecosystem and malware compared to previous methods. The book also introduces an ensemble multi-class classifier scheme to classify malware into known families. Furthermore, we propose a novel framework of mapping malware to vulnerabilities exploited using Android malware's behavior reports leveraging pre-trained language models and deep learning techniques. The mapped vulnerabilities can then be assessed on confidentiality, integrity, and availability on different Android components and sub-systems, and different layers.

175,60 €
175,60 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9781032407463
Medium: Buch
ISBN: 978-1-032-40746-3
Verlag: CRC Press
Erscheinungstermin: 17.08.2023
Sprache(n): Englisch
Auflage: 1. Auflage 2023
Produktform: Gebunden
Gewicht: 458 g
Seiten: 189
Format (B x H): 161 x 240 mm