Book Review

Mobile Platform Security

N. Asokan, Lucas Davi
Alexandra Dmitrienko, Stephan Heuser, Kari Kostiainen
Elena Reshetova and Ahmad-Reza Sadeghi

Increased mobile applications call for the extensive knowledge in realizing the security and management capabilities of various mobile platforms. It is evident that the existing mobile platforms are prone to security vulnerabilities and management limitations. A few ones are considered as more mature than others with regard to supporting the most appropriate set of policies required by the different mobile roles within the organization.

The research carried out in the mobile security has been documented in the literature widely. The current compendium is an illustration of the new progress in the mobile security.

This book has eight chapters besides bibliography.

The authors have given the mobile security history before presentation of chapter divisions. Besides they presented the current mobile security environment as a prelude to the work.

The security platform design considers a few components such as stakeholders where each one has a role and their functions have impact in designing. To build up a secured software architecture the authors have given a good proposition. This chapter has given a comprehensive focus on preliminaries.

In the third chapter, the authors have detailed different mobile platforms. The security architecture behind every platform is studied with good amount of crucial issues. The mobile platforms presented in the previous chapter are now compared with features. To do so they have used the security architectures proposed in the chapter 2 which lead the book to a well structured presentation. Some required bases such as authentication runtime protection and application protection are given.

In the chapter 5, they have detailed the hardware security mechanisms. The discussed issue such as platform integrity, and continue to device identification, secure storage, isolated execution, and device authentication in this chapter have contributed to the themes. In the later part of the chapter they listed the existing architectures and emerging standards for deployment of hardware security mechanisms in mobile devices.

The commercial security extensions are discussed in the chapter on Enterprise security extensions in the next chapter. In the penultimate chapter, the authors have explained the current research on security platform with many supporting architectures.

They concluded briefly with a long list of extensive bibliography.

The book is marked by a very systematic presentation and well planned structure. The plan as given in the second chapter is followed which enable the users for good understanding on mobile security issues. Hope this book will serve as a good initiative point for the readers in mobile security.

Yuxin Mao
School of Computer and Information Engineering
Zhejiang Gongshang University, Hangzhou, P.R China