Chapter 85
Security in Mobile Computing

Venus W. Samawi
Amman Arab University, Jordan

ABSTRACT

These days, peoples expected to move around carrying their mobile devices, talking to friends, completing their work, accessing emails etc. His/her pictures, work, study, even relationship (friends, and family) all is in the mobile device. Therefore, mobile devices (especially smart phones) become an ideal target for different attacks. Mobile computing also becomes important in enterprises and organizations. Therefore, it is important to illustrate the state of art on vulnerabilities and threats on mobile device. This chapter is addressed to explain mobile computing concept, features, architecture, operating systems, and risks to mobile devices. Mobile operating system structure and characteristics are demonstrated. The author also illustrates mobile security issues, and type of threats to mobile devices. Finally, features and security models of two popular smartphone operating systems, Android and iOS, are illustrated. It was found that the security models of these two smartphones is immature and do not meet the enterprises security policies.

INTRODUCTION

Recent advances of hardware and software in mobile computing contributed to the improvement of services delivered by institutes, enterprise and government organizations. Business that had to stop when the employees leave their desks now is supplemented by using mobile devices (smartphones, PADs, wireless ultra-books and laptops). Most of the corporate employees in these organizations use mobile devices to access, find, share information, and perform email communication at any time and from any place. In this chapter, we will emphasis on smartphones due to the explosive growth and increasing usage of these devices.

The main aspect of mobile computing is portability, which requires software (mobile application requirements, and data encryptions), hardware (mobility devices and components), and mobile communication issues (network infrastructure, protocols, and communication properties) (Agrawal et al, 2003; Nosrati et al, 2012). Mobile devises should be equipped with a suitable operating system to run its services and to act as a platform that organizes the mobile device functionalities.

Although we benefit from numerous services provided by mobile computing, we must understand that we are the victims of security vulnerabilities (Agrawal et al, 2003). Mobile computing

needs extra security issues compared with other computer networks. This is due to the additional constraints caused by wireless transmission and mobility characteristics.

In this chapter, we are keen on answering the following questions: What does mobile computing mean? What are its main characteristics? Does it need special form of operating system? Is it more vulnerable to attacks? What are the main security issues in mobile computing? What are the main security problems that need to be solved?

MOBILE COMPUTING

Mobile computing is a term that refers to a set of computing operations that allows information accessing anytime, from any place, using any mobile device (laptops, tablets, or smartphones). If the information to be accessed is local, then the user is working under disconnected mode operation. When the device is connected to a network through wireless or wired connection, in this case the user is working under connected mode. Nowadays, mobile devices play an essential role in human daily lives. This is attributed to the availability of different forms of mobile communications (viz. 3G, 4G, GPRS, Bluetooth and Wi-Fi) that enable users to access various ubiquitous services regardless of time (Deepak & Pradeep, 2012). The main challenges faced by the mobile devices are limitation of their resources (viz. battery life, storage, and bandwidth) which affect the service qualities and communications (viz. mobility and security).

The availability of small powerful computing devices, improved telecommunication and specialized software helped the prevalence process of mobile computing (Deepak, 2012). The main mobile computing characteristics are common with other technologies. But they are of special importance to the mobile computing (Agrawal et al, 2003; Deepak & Pradeep, 2012; Nosrati et al, 2012).

- **Portability:** The ability of the device to operate consistently during its move. It can operate at any time and in any place. Therefore, rechargeable batteries are needed to support working for several hours without needing any external charger

- **Data Connection:** The networking infrastructure that allows digital connection to the Internet for transmitting and receiving data. Mobile connectivity could be cellular connection (GSM, CDMA or GPRS, 3G, and 4G networks), WiFi connection (accessed through a private business network or through public hotspot), or Satellite Internet access.

- **Social Interactivity (Interactivity):** The collective cooperation and data exchanging between users.Here, data denotes files transfer, emails, facsimile, and accessing WWW. Interactivity is more important for mobile devices, since they have less computing power than other types of technology.

- **Individuality:** A basic component in mobile computing, which providing communication services between individuals. Basically, mobile devices are designed for individuals

Mobile computing devices suffer from series of specific problems and limitations. In brief, could be described as follows (Nosrati et al, 2012; Deepak & Pradeep, 2012):

- **Scarcity of Bandwidth:** In mobile computing, users need to access Internet on the move. In this case, we need sort of wireless connectivity (cellular, WiFi, or Satellite), which could be a weak point. If we are not near any of these connections, accessing the internet will be very limited.

- **Security Standards:** Most people nowadays keep their private sensitive information on their mobile devices. They connect

Related Content

Design of Medium Power Amplifier Using GaAs PHEMT Technology for Wireless Applications
Amiza Rasmi (2012). *Advances in Monolithic Microwave Integrated Circuits for Wireless Systems: Modeling and Design Technologies (pp. 185-204).*
www.irma-international.org/chapter/design-medium-power-amplifier-using/58492

An Advanced and Secure Symbian-Based Mobile Approach for Body Sensor Networks Interaction
Orlando R. E. Pereira, João M. L. P. Caldeiraand Joel J. P. C. Rodrigues (2012). *Wireless Technologies: Concepts, Methodologies, Tools and Applications (pp. 1061-1077).*
www.irma-international.org/chapter/advanced-secure-symbian-based-mobile/58830

Detection of PUE Attack in CRN with Reduced Error in Location Estimation Using Novel Bat Algorithm
Aasia Rehmanand Deo Prakash (2017). *International Journal of Wireless Networks and Broadband Technologies (pp. 1-25).*
www.irma-international.org/article/detection-of-pue-attack-in-crn-with-reduced-error-in-location-estimation-using-novel-bat-algorithm/201494

Secure Node Localization in Mobile Sensor Networks
Rachit Mittaland Manik Lal Das (2014). *International Journal of Wireless Networks and Broadband Technologies (pp. 18-33).*
www.irma-international.org/article/secure-node-localization-in-mobile-sensor-networks/104628

The Impact of Standards in Web Services Security
Pauline Ratnasingam (2014). *International Journal of Wireless Networks and Broadband Technologies (pp. 21-39).*
www.irma-international.org/article/the-impact-of-standards-in-web-services-security/115588