Chapter 3
Conservation of Mobile Data and Usability Constraints

Rania Mokhtar
University Putra Malaysia (UPM), Malaysia

Rashid Saeed
International Islamic University Malaysia (IIUM), Malaysia

ABSTRACT

An important part of ISO/IEC 27002 cyber security standard is the conservation of confidentiality that falls under its computer facility protection part which insures that the computer and its stored information can only be accessed by the authorized users. Securing mobile devices and mobile data to ensure the confidentiality, integrity, and availability of both data and security applications requires special consideration to be paid to the typical mobile environment in which a mobile computing device would be utilized. Protecting mobile devices includes multiple security technologies such as the right identification of its particular user, data encryption, physical locking devices, monitoring and tracking software, and alarms. This chapter reviews security-specific hardware and software applied to mobile computing and presents its advantages and drawbacks. Then it considers the concept of usability constraints in context of mobile computing security and introduces the seamless security method for identity proof of a particular user or device.

DOI: 10.4018/978-1-60960-851-4.ch003

INTRODUCTION

Within the much broader arena of cyber security, organizations may be able to provide the physical and environmental security but this does not cover the mobile data that is stored in mobile devices including mobile computing devices such as laptops and palmtops and mobile storage devices such as USB drives. Several laptop manufacturers, such as Acer, Compaq, MPC and IBM, have added security focus features to certain models. Other vendors have focused on augmenting laptop vendor's systems with hardware-based encryption engines, such as CryptCard, and security-specific authentication and encryption software, such as SafeBoot (Sharp 2004).

Scantily administered mobile computing devices significantly raise the possibility for security failures and data compromise. Stolen or lost mobile computing/storage device carrying restricted data, such as secret e-mails, customer data and financial reports, pose the risk of falling into the wrong hands. The loss of highly restricted data and the potential connected media scandal is a massive problem in itself, but the impact might be greater if failure to protect certain sensitive data can be interpreted as a defiance of regulations. Security requirements for the protection of sensitive mobile data in mobile computing context are still lacking in the current literature of cyber security. The purpose of this chapter is twofold; address the mobile computing security policies within the map of cyber security requirements and investigate the seamless security tools and mechanisms that take into account user's usability constraints.

BACKGROUND

Most initial mobile computing devices were considered useful, but not something to be protected. This continued for a number of years until the importance of mobile data was truly realized. When mobile computing applications were developed to handle secure organizational and personal data, the real need for mobile data security was felt like never before. It's been realized that mobile data on mobile computing devices is an extremely important aspect of modern life.

Mobile computing is realized strongly and has become very trendy because of the expediency and portability of mobile computing devices. Mobile computing devices are responsible for employees to store, process, transmit, or access organizations restricted data. The use of mobile computing devices provides flexibility and enhanced communications that allow organizations to be more productive.

In some organizations, the notebook has eclipsed the desktop as the standard computing platform in order to enable employees to take their work home with them and maximize productivity. In others, personal data assistants are the computing platform de jour. But organizations need to put the proper tools in place to ensure that their mobile devices and networks are not compromised as a result of this increase in mobility. However, mobile computing creates threats to the stored mobile data and fixed devices/data based on their ability for internet connectivity to static resources and/or upon their intranet connectivity e.g. virus spreading which lacks the internal protections afforded by organization such as firewalls. Protecting the mobile computing devices and the sensitive data they may store or have access to be critical security issue that must be addressed (security policies 4-007, 2007).

Various threads and risks intimidate the mobile computing devices in different degrees, such as:

- Threatened by loss or thievery defined as physical hazard.
- Illegal access risk. Accessing the device by an illegitimate user.
- Foreign network risk. Mobile computing devices may use different networks connection in the move. Although all networks