

Chapter 7.5

Securing Mobile Data Computing in Healthcare

Willy Susilo

University of Wollongong, Australia

Khin Than Win

University of Wollongong, Australia

ABSTRACT

Access to mobile data and messages is essential in healthcare environment as patients and healthcare providers are mobile. This is inline with the need of ubiquitous computing in everyday life. Mobile and wireless devices can assist in ensuring patient's safety by providing easy availability of the data at the point of care. Portability and accessibility of these devices enhances use of them in healthcare environment. However, data integrity and confidentiality of information in them need to be ensured to provide safe, effective and efficient healthcare. Mobile healthcare involves conducting healthcare related activities through using mobile devices such as a smart phone,

Personal digital assistant (PDA), wireless enabled computer, iPod and so on. Mobile computing is suitable for healthcare as healthcare providers are mobile. These would be suitable for conducting patient's healthcare activities in emergencies, ward rounds, homecare, chronic disease management, conducting clinical trials, and so on. There are various projects using mobile devices to enhance patient's care. With the advancement of medical informatics, telemedicine and information technology, mobile data devices play an enormous role in healthcare system. In this chapter, we outline the need of mobile devices in healthcare, usage of these devices, underlying technology and applications, importance of security of these devices, securing mobile data communication

in healthcare through different security models and case examples of applications that we have developed, in particular (1) iPathology tool on iPod, (2) securing healthcare information using Pocket PC 2003, and (3) securing information on handheld devices. There were several incidents in the past due to the insecurity of mobile devices that can leak information to anyone who does not have access to the information. In this chapter, we will illustrate several techniques that we have developed to protect these malicious activities and how these are applicable for securing mobile data computing in healthcare.

INTRODUCTION

In recent years, a wide range of handheld devices have been introduced in the market. Pocket size handheld organizers, called personal digital assistants (PDAs), have evolved from offering simple services such as calendar, address book, and e-mail, to working as a powerful mobile network client that can be used to access corporate databases and be used as part of an e-commerce platform. The healthcare industry is not an exception with healthcare providers using various handheld devices for accessing information and for telemedicine purposes. These days, the mobile devices are also equipped with communication abilities, such as GSM/GPRS ability, WiFi 802.11a/b/g Wireless LAN or Bluetooth. Handheld devices are perfect for carrying information, such as multimedia information, on the fly. Users can enjoy the information while they are on their way to work, etc.

Securing such devices includes providing protection for wireless communication, stored data and against viruses and malicious codes, together with making provisions for preventing theft of the device. The more we become dependent on handheld devices, the more threatening the attack will be. Today the U.S. military is already relying extensively on such devices. These devices can be

used for GPS, viewing maps of areas, interacting with other troop units and as (remote) sensors (such as those used against bio-warfare), etc. Moreover, the U.S. military is spending large amounts of money to expand the capabilities of such devices. Other applications in critical infrastructures can be expected. For example, today many firefighters and ambulance services rely on paper maps. In regions in the world that expand rapidly, there is a significant advantage to switch to handheld devices where maps are updated more frequently. Since several manuals are primarily available via the Internet, handheld devices will be used by technicians to repair machinery in nuclear power plants, airplanes, etc.

There are several major differences between a desktop computer and a handheld device including limited input methods, small screen size, lower range processor, and limited memory for the handheld device. These differences affect the design of applications that run on these devices. Palm OS and Pocket PC handheld devices do not have a keyboard. Although a third party keyboard, such as Palm Portable keyboard or Targus Stowaway keyboard, can be used, most users enter text to the device with a *stylus* which is then recognised by a character recognition program such as Palm *Graffiti* or *Microsoft Transcriber*. Other methods of input include using the on-screen keyboard, or typing text on a desktop PC that is connected to the PDA. Communication with the device is achieved by using the HotSync/ActiveSync that synchronizes the data with its copy that is stored on a desktop computer, using a communication port such as the serial port, the IrDA (Infrared Data Association) port, or the USB port.

Palm 1000 was introduced by 3Com in 1996. Devices running Palm OS have dominated the handheld market and currently having around 70% of the market share (Hansmann, Merk, Nickous, & Stober, 2001). Palm OS is also adopted by companies such as HandSpring and IBM with applications ranging from Palm OS native applications including Address Book

8 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/securing-mobile-data-computing-healthcare/26347

Related Content

A Human-Like Cognitive Computer Based on a Psychologically Inspired VLSI Brain Model

Tadashi Shibata (2013). *Technological Advancements in Biomedicine for Healthcare Applications* (pp. 247-266).

www.irma-international.org/chapter/human-like-cognitive-computer-based/70868

A Computer Aided Diagnostic Tool for the Detection of Uterine Fibroids

N. Sriraamand L. Vinodashri (2013). *International Journal of Biomedical and Clinical Engineering* (pp. 26-38).

www.irma-international.org/article/a-computer-aided-diagnostic-tool-for-the-detection-of-uterine-fibroids/96826

Visual-Tactile Bottom-Up and Top-Down Attention

Qiong Wu, Chunlin Li, Satoshi Takahashiand Jinglong Wu (2013). *Biomedical Engineering and Cognitive Neuroscience for Healthcare: Interdisciplinary Applications* (pp. 183-191).

www.irma-international.org/chapter/visual-tactile-bottom-top-down/69918

Finding Impact of Precedence based Critical Attributes in Kidney Dialysis Data Set using Clustering Technique

B.V. Ravindra, N. Sriraamand Geetha Maiya (2015). *International Journal of Biomedical and Clinical Engineering* (pp. 44-50).

www.irma-international.org/article/finding-impact-of-precedence-based-critical-attributes-in-kidney-dialysis-data-set-using-clustering-technique/136235

A Romance of the Three Kingdoms: Biotechnology Clusters in Beijing, Shanghai and Guangdong Province, China

Petr Hanel, Jie He, Jingyan Fu, Susan Reidand Jorge E. Niosi (2017). *Comparative Approaches to Biotechnology Development and Use in Developed and Emerging Nations* (pp. 67-129).

www.irma-international.org/chapter/a-romance-of-the-three-kingdoms/169515