Chapter 13
Wireless Identity Management: Multimodal Biometrics and Multilayered IDM

Abdullah Rashed
University of Minho, Portugal

Henrique Santos
University of Minho, Portugal

ABSTRACT

In the wireless era, digital users in the electronic world (e-world) are represented by sets of data called Digital Identities (ID), which they use, among other functions, for authentication purposes. Within the e-world it is risky to lose an identity and so security solutions are required to protect IDs. Information security should provide the necessary Identity Management (IDM) process to mitigate that threat. Moreover, efficient protection of digital identities would encourage users to enter the digital world without worries. The suggested solution depends on three dimensions: management, security solution, and security dimensions. The proposed model appears as a multi-layered security approach, since it tries to integrate different security technologies and multimodal biometrics tools and practices, such as wireless management, policies, procedures, guidelines, standards, and legislation. The advantages, limitations, and requirements of the proposed model are discussed.

INTRODUCTION

Wireless network and mobility have laid the foundation for a new era of computer users (Higby & Bailey, 2004), especially in Internet arena, and generated a lot of wireless clients everywhere (Yan, et al., 2009). This growth of the Internet has made it an integral part of many businesses’ daily operations (Taylor, 2001). Today’s user desires both flexibility and mobility (Keshariya & Hunt, 2008). The growth in the popularity of Internet services, increasing demands of mobile users together with a wide range of access technologies and mobile-networked devices, demands integration and inter-working of these heterogeneous access networks (Keshariya & Hunt, 2008). However,
this popularity has not been as eagerly received by network administrators. Because a great majority of these users lack the knowledge and/or experience to implement best practices, such as installing the latest security patches and antivirus software protection, or properly configuring firewalls, small networks are experiencing high levels of unwanted malicious activity (Yan, et al., 2009). Therefore, securing wireless networks in an untrustworthy open environment is always a challenging problem (Boudriga, et al., 2006). Network has facilitated some security vulnerabilities and malicious attacks. Even with good internal security practices, such as firewalls and virus protection, small networks are still vulnerable to malware, since wireless access on small networks allows the spread of computer viruses and worms due to laptops moving between campus and less-protected networks (Yan, et al., 2009). Distributed security management would be used for preventing malicious behaviours (Boudriga, et al., 2006).

To enter the e-world users have to use some sort of credentials (ID) as shown in Figure 1. Authentication is a process of two different actions: provision and verification (Sklavos, et al., 2007) as shown in Figure 2.

Due to its fast and networked nature, e-world can provide that information for non expected purposes, such as business communications and marketing (Casassa & Thyne, 2006). Moreover, given the lack of face to face interaction, stolen or lost credentials can be easily abused to hide many types of e-crimes. Besides, users might be

Figure 1. Authentication process

Figure 2. A three-party authentication model (Sklavos, et al., 2007)