Chapter 19
Preserving the Privacy of Patient Records in Health Monitoring Systems

Mahmoud Elkhodr
University of Western Sydney, Australia

Seyed Shahrestani
University of Western Sydney, Australia

Hon Cheung
University of Western Sydney, Australia

ABSTRACT

The goal of this chapter is to discuss the challenges of generic security protocols and platforms for securing Electronic Health Records (EHR) in general and for their adoption in shared care environments in particular. The chapter introduces various methods and security solutions based on existing protocols, discusses their potentials, and describes some experiences with their implementations. Amongst the main challenges that e-health technology faces, security is considered as one of the major obstacles to its deployment. The chapter proposes an authentication approach, referred to as Ubiquitous Health Trust Protocol (UHTP), which aims at minimizing the security risk associated with the remote access of EHRs using portable devices. In particular, the proposed approach has been used to create ways for secure collaboration providing a set of generic services such as read/write, authentication, and trust management, as well as advanced functionality for mobile access. The experience in adopting the approach using Java on the Android platform is described.

INTRODUCTION

While the history of cryptography began thousands of years ago, academic research into computer cryptography can only be dated back to mid-1970s (D'Agapeyeff, 2008). Some of the earlier research on modern cryptography can be attributed to IBM which designed an algorithm that became the US Federal Data Encryption Standard (Smid & Branstad, 1988). Typically, cryptography has been used as a tool to generally secure communications and computer systems.

DOI: 10.4018/978-1-4666-4030-6.ch019

Recently, modern cryptography has been extended to a wide range of techniques. Credit cards with smart-card capabilities equipped with the power to execute cryptographic programs are some of the popular applications in use today. In Engineering, cryptography becomes more complicated by encompassing cryptographic theories with computer engineering hardware design and computer software algorithms. Visual cryptography is another technique used to allow visual information, such as text and images, to be encrypted in a way that decryption does not requires a computer system (Naor & Shamir, 1995). But perhaps, public-key cryptography and symmetric-key cryptography are among the popular techniques in use today. Symmetric-key cryptosystems use the same key for the encryption and decryption of a message. This was the only type of encryption publicly known until 1976 (Diffie & Hellman, 1976). A significant disadvantage of symmetric encryption is the management of keys, especially for applications on the Internet. Nevertheless, research into cryptographic techniques has been extended to include quantum physics. Quantum cryptography represents a new paradigm for securing communications systems since its security is based on the laws of quantum physics and not only on computations (Ekert, 1991). Collaborations between, mathematicians, electrical engineers, physicians, computer scientists and others have led to the state-of the-art design of various cryptography applications and the incorporation of security techniques in various applications such as in the domain of e-health. One of the major concerns with e-health systems relates to their capabilities in preserving the privacy of the patients and their medical records, which may contain highly sensitive and confidential personal information.

Electronic Health Record (EHR) provides an advanced scheme for maintaining patients' records across distributed health information systems and other health networks (B. Blobel, 2006). Compared to traditional paper-based record systems, EHRs are more efficient and reliable, providing higher degrees of availability (Hillestad, et al., 2005). But privacy and security concerns have foiled their widespread acceptance and use. To address these concerns, cryptography-based solutions have already been suggested by some researchers (Petković, Katzenbeisser, & Kursawe, 2007). But for the successful deployment of e-health systems, provision of comprehensive security measures for medical information remains a challenge that needs to be met. Cryptography is an essential element for addressing this challenge and hence the widespread acceptance of e-health systems.

Most cryptography-based solutions provide secure communication mediums for use by e-health systems (Barua, Liang, Lu, & Shen, 2011). The approaches proposed in this Chapter, use and expand such solutions. They ensure that an EHR, for instance maintained in some remote health monitoring system, is only disclosed to the authorized healthcare professionals, on their registered devices, only at the valid locations, and over a secure channel. To achieve these, building on the strengths of Transport Layer Security (TLS) protocol, a trust negotiation approach is proposed. For verification purposes, a mobile application is also constructed. The experimental works confirm that by applying the proposed approach, significant improvements in the security of the remote health monitoring systems can be achieved. The improvements in the security of the remote monitoring systems are achieved by, not only securing the communication channel, but also by providing extra protective features to the access control and authorization process before the release of any data over unsecured network. This is an enhancement to the traditional identity based only authentication's techniques.

E-Health Views and Challenges

The healthcare industry is under continuous development and growth. In the 2008–09 financial year, there were 8.1 million patients admitted to hospitals in Australia (Australian Hospital, 2010).