Chapter 1
Secure Exchange of Electronic Health Records

Alejandro Enrique Flores
University of Wollongong, Australia

Khin Than Win
University of Wollongong, Australia

Willy Susilo
University of Wollongong, Australia

ABSTRACT

Protecting the confidentiality of a patient's information in a shared care environment could become a complex task. Correct identification of users, assigning of access permissions, and resolution of conflict rise as main points of interest in providing solutions for data exchange among health care providers. Traditional approaches such as Mandatory Access Control, Discretionary Access control and Role-Based Access Control policies do not always provide a suitable solution for health care settings, especially for shared care environments. The core of this contribution consists in the description of an approach which uses attribute-based encryption to protect the confidentiality of patients' information during the exchange of electronic health records among healthcare providers. Attribute-based encryption allows the reinforcing of access policies and reduces the risk of unauthorized access to sensitive information; it also provides a set of functionalities which are described using a case study. Attribute-based encryption provides an answer to restrictions presented by traditional approaches and facilitate the reinforcing of existing security policies over the transmitted data.

INTRODUCTION

In a shared care paradigm, remote access to distant data repositories along with the exchange of relevant electronic health records (EHRs) becomes essential for providing integral health care services. Internet is the natural platform to support such functionalities. However, the insecure nature of the network and the increased amount of health information transmitted through it raise the concern over the secure exchange of EHRs (Ohno-Machadoa, Silveira, & Vinterbo, 2004). In fact, the disclosure, transmission and use of a patient's data for delivering health care services

DOI: 10.4018/978-1-61692-895-7.ch001

are an expanding practice that concerns the interest of health institutions, physicians and patients. In a dynamic and demanding environment, such as health care, a patient's confidentiality can only be guaranteed by incorporating security services and mechanisms along with common security policies and/or conflict resolution policies to protect the data at any given point (Lopez & Blobel, 2009). Additionally, EHR systems not only should assure the protection of patients' privacy and confidentiality but also guarantee the reliability and integrity of the information gathered by health care professionals (Conrick & Newell, 2006). Therefore, it is essential that health information systems consider the privacy and integrity of the data and also allow the safe retrieval of information for primary and secondary uses, especially in an interconnected health information scenario (Lusignan, Chan, Theadom, & Dhoul, 2007).

In this context, projects centered in the interconnection of health information systems, such as national health information initiatives or multi-domain EHR systems, not only confront information and functional requirements, such as the development and implementation of standardized communication protocols, standardized vocabulary and homogeneous development frameworks, but also privacy and security requirements. Protection of a patient's privacy and the secure disclosure of health information are crucial functionalities that should be embedded within the specifications of modern and reliable electronic health record systems (Conrick & Newell, 2006; Ohno-Machadoa, et al., 2004; Safran, et al., 2007). Moreover, to guarantee the secure transmission and release of health information in a shared care paradigm, the protection of a patient's privacy has to be conceived as an issue which combines the secure transmission of data, correct user authentication, access control and security policies, either at the point of origin or at the destination of the communication channel.

During the exchange of EHRs, even when the transmission has been between trusted parties, access permission can be violated under specific circumstances. Consider a scenario in which health care institutions A and B are trusted parties during the exchange of information. Using public key technologies both institutions can transmit information using a secure channel. The secure channel guarantees confidentiality and integrity of the transmitted information. However, the existence of different access policies may lead to a violation of access permissions either at the point of origin or when the information reaches its destination. Blobel et al. have suggested the definition of common domain policies to address differences or conflicts rising from disparities in the definition of security and access policies existing among health care organizations (Blobel, Nordberg, Davis, & Pharow, 2006). However, implementing this approach requires the existence of standardized vocabularies and common policy structures, which is limited in the actual health information infrastructure. There is also a virtual agreement that for communication of medical information and posterior access to the data, access policies based on role-based access control models may facilitate the overcoming of possible violation of access permission (Blobel, et al., 2006; Gritzalis & Lambrinoudakis, 2004). However, role-based access control models also present issues that may increase the risk of unauthorized access to sensitive medical data (Alhaqbani & Fidge, 2008).

This chapter aims to address the issues of secure transmission of data, access control and user privileges and propose a specification for an information exchange model that allows a secure and safe approach for the exchange and release of EHRs in a shared care scenario. Assuming that transmission of medical information is maintained over insecure channels, we propose a policy reinforcement model based on attribute-based encryptions and incorporate security mechanisms in order to protect patients' privacy during the exchange and release of the information.