Chapter 2.11

Exploring Type-and-Identity-Based Proxy Re-Encryption Scheme to Securely Manage Personal Health Records

Luan Ibraimi
University of Twente, The Netherlands

Qiang Tang
University of Twente, The Netherlands

Pieter Hartel
University of Twente, The Netherlands

Willem Jonker
University of Twente, The Netherlands

ABSTRACT

Commercial Web-based Personal-Health Record (PHR) systems can help patients to share their personal health records (PHRs) anytime from anywhere. PHRs are very sensitive data and an inappropriate disclosure may cause serious problems to an individual. Therefore commercial Web-based PHR systems have to ensure that the patient health data is secured using state-of-the-art mechanisms. In current commercial PHR systems, even though patients have the power to define the access control policy on who can access their data, patients have to trust entirely the access-control manager of the commercial PHR system to properly enforce these policies. Therefore patients hesitate to upload their health data to these systems as the data is processed unencrypted on untrusted platforms. Recent proposals on enforcing access control policies exploit the use of encryption techniques to enforce access control policies. In such systems, information is stored in an encrypted form by the third party and there

DOI: 10.4018/978-1-60960-561-2.ch211

is no need for an access control manager. This implies that data remains confidential even if the database maintained by the third party is compromised. In this paper we propose a new encryption technique called a type-and-identity-based proxy re-encryption scheme which is suitable to be used in the healthcare setting. The proposed scheme allows users (patients) to securely store their PHRs on commercial Web-based PHRs, and securely share their PHRs with other users (doctors).

INTRODUCTION

Recently, healthcare providers have started to use electronic health record systems which have significant benefits such as reducing healthcare costs, increasing the patient safety, improving the quality of care and empowering patients to more actively manage their health. There are a number of initiatives for adoption of electronic health records (EHRs) from different governments around the world, such as the directive on privacy and electronic communications in the U.S. known as the Health Insurance Portability and Accountability Act (HIPAA) (The US Department of Health and Human Services, 2003), which specify rules and standards to achieve security and privacy of health data. While EHR systems capture health data entered by health care professionals and access to health data is tightly controlled by existing legislations, personal health record (PHR) systems capture health data entered by individuals and stay outside the scope of this legislation. Before going into details on how to address the confidentiality issues, let us introduce the definition of PHR system (The personal health working group final report, 2004):

"An electronic application through which individuals can access, manage and share their health information, and that of others for whom they are authorized, in a private, secure, and confidential environment."

PHR systems are unique in their design since they try to solve the problem that comes from scattering of medical information among many healthcare providers which leads to unnecessary paper work and medical mistakes (The personal health working group final report, 2004). The PHR contains all kinds of health-related information about an individual (say, Alice) (Tang, Ash, Bates, Overhage & Sands, 2006). Firstly, the PHR may contain medical data that Alice has from various medical service providers, for example about surgery, illness, family history, vaccinations, laboratory test results, allergies, drug reactions, etc. Secondly, the PHR may also contain information collected by Alice herself, for example weight change, food statistics, and any other information connected with her health. Controlling access to PHRs is one of the central themes in deploying a secure PHR system. Inappropriate disclosure of the PHRs may cause an individual serious problems. For example, if Alice has some disease and a prospective employer obtains this, then she might be discriminated in finding a job.

Commercial efforts to build Web-based PHR systems, such as Microsoft HealthVault (Microsoft, 2007) and Google Health (Google, 2007), allow patients to store and share their PHRs with different healthcare providers. In these systems the patient has full control over her PHRs and plays the role of the security administrator - a patient decides who has the right to access which data. However, the access control model of these applications does not give a patient the flexibility to specify a fine-grained access-control policy. For example, today's Google Health access control is *all-or-nothing* - so if a patient authorizes her doctor to see only one PHR, the doctor will be able to see all other PHRs. Another problem is that the data has to be stored on a central server locked by the access control mechanism provided by Microsoft HealthVault or Google Health, and the patient loses control once the data is sent to the server. PHRs may contain sensitive information such as details of a patients disease, drug usage,