Chapter VII

Towards a Secure Web-Based Healthcare Application

Konstantin Knorr
University of Zurich, Switzerland

Susanne Röhrig
SWISSIT Informationstechnik AG, Switzerland

INTRODUCTION

In healthcare a lot of data are generated that in turn will have to be accessed from several departments of a hospital. The information kept within the information system of a hospital includes sensitive personal data that reveal the most intimate aspects of an individual’s life. Therefore, it is extremely important to regard data protection laws, privacy regulations, and other security requirements. When designing information systems for healthcare purposes, it is an imperative to implement appropriate access control mechanisms and other safeguards. Furthermore, a tendency to use the Internet as a communications media can be observed. As the Internet is an insecure transmission media, the security requirements that must be met by the overall system are high.

During the project MobiMed (Privacy and Efficiency of Mobile Medical Systems; further information about the project can be found at http://www.ifi.unizh.ch/ikm/MobiMed/), a prototype was developed to show the feasibility of the implementation of security mechanisms required in a Web-based healthcare application.
This chapter describes the specific security requirements in healthcare environments, focusing on the additional security demands resulting from the use of the Internet as a communications media.

**RELATED WORK**

The technical committee 251 of the European Committee for Standardization is responsible for medical informatics. Working group 6 focuses on standardization in healthcare concerning security, privacy, quality and safety. The safety of systems is defined as “the expectation that systems do not, under defined conditions, enter a state that could cause human death or injury.” We will not discuss “safety” in this chapter, but focus on “security” instead, whose definition is the subject of the next section *General Security Objectives*.

Rindfleisch (1997) gives a general introduction of privacy aspects and security measures in healthcare. Anderson (1996b) introduces a security policy model for clinical information systems which makes use of nine principles. The policy is compared to traditional policies from the banking and military sectors. Traditionally, security requirements in healthcare environments are high. Especially since the rise of global networks a lot of attention has been paid to this topic. Baker and Masys (1999), Rind (1997), and Blobel (1997) present distributed systems and networks in healthcare regarding security aspects focusing on confidentiality and privacy.

The prototype that will be introduced in this chapter is based on a clinical process. Healthcare processes and their support through information and communication technology have recently received much attention. Scheer, Chen and Zimmermann (1996) discuss the process management in a hospital. Knorr, Calzo, Röhrig and Teufel (1999) describe the modeling and redesign of a clinical process. Kuhn, Reichert and Dadam (1995), Yousfi, Geib and Beuscart (1994), Reichert, Schultheiss and Dadam (1997), and Bricon-Souf, Renard and Beuscart (1998) introduce, discuss and analyze workflow management systems and their impact on healthcare.

Nevertheless the above publications focus only on specific security objectives. Unlike these approaches we take a general and structured outlook on the problem and take into account the four major security objectives: confidentiality, integrity, availability, and accountability. These objectives and their special meaning in healthcare systems are regarded, specifically for data transmission and storage. A prototype shows possible security measures and the feasibility of their implementation.
Patients with a Spinal Cord Injury Inform and Co-Construct Services at a Spinal Cord Rehabilitation Unit
[www.igi-global.com/chapter/patients-spinal-cord-injury-inform/49265?camid=4v1a](www.igi-global.com/chapter/patients-spinal-cord-injury-inform/49265?camid=4v1a)