Chapter 7
Statistical Models for EHR Security in Web Healthcare Information Systems

Stelios Zimeras
University of the Aegean, Greece

Anastasia N. Kastania
Athens University of Economics & Business, Greece

ABSTRACT

Security is an important requirement for health information systems. Security is important for several reasons, most of which have a foundation in economics. Firstly, equipment is expensive to get, install, and integrate into the infrastructure of an organization. Secondly, the operations of an organization are based on the applied technology infrastructure, which means that disruption of operations quickly turns into unnecessary costs and, when applicable, potential loss of revenue. The adoption of digital patient records, increased regulation, supplier consolidation, and the increasing demand for information, highlights the need for better information security. Electronic health (e-Health) has become an important area of concern. A comprehensive EHR (Electronic Health Record) at the point of care could be created by collecting and sharing data among all sites at which patient receives care, as well as by incorporating information supplied by the patient. One of the greatest incentives to adopting EHRs will be reaching a critical mass of information sharing investors in health care information technology. In this work the authors examine the security properties of the EHR, with a special emphasis on software reliability. The authors focus on modelling and studying the reliability feature of the EHR. Special attention is given on exploiting the mathematical foundations of reliability modelling in a service-oriented architecture. Statistical measures called web metrics can be introduced to assess the performance of these systems.

INTRODUCTION

Security and privacy are important requirements for health information systems. During the last decade much attention has been given to the different aspects of information systems security. Security is important for several reasons: (1) equipment is expensive to buy, install, and integrate into the infrastructure of an organization; (2) the operations of an organization are dependent on

DOI: 10.4018/978-1-61692-895-7.ch007

applied technological infrastructure, which means that disruption of operations quickly turns into unnecessary costs and potential loss of revenue and (3) laws in most computer-dependent nations enforce protection of data and proprietary information stored on computer systems.

Every feature of health care and the medical profession is penetrated by computing and networking architectures. An issue of growing importance in the healthcare sector is information security and privacy. The EHR (Electronic Health Record), as defined by Cambridge Health Informatics Ltd (2001), is a summary lifelong record holding electronically details of potentially all of patient's interactions with the healthcare system (Singleton et al, 2001). A comprehensive EHR at the point of care could be created by collecting and sharing data among all points of care, where a patient is treated, as well as by integrating data supplied by the patient. Data must be built on common words (data and terminology), structures and organizations (in terms of interoperability) in order to be shared and used by possibly heterogeneous institutions. A growing body of research is focused on developing mechanisms to address privacy and security concerns related to Internet and mobile healthcare applications.

Using composition in designing and building software systems is one of the distinguishing features of the component-based and service-oriented approaches. Reliability is a particular expression of the broader concept of dependability. Other dependability aspects are, for example, availability and safety. The quality of the flow of service delivered by a system is referred to as reliability. In the literature two definitions of reliability exist: (i) the probability that the system performs its proper functions under specified conditions of time and (ii) the probability that the system successfully completes its operation when it is invoked (also known as "reliability on demand").

In this work we focus on studying and modelling the reliability of Web applications for healthcare, which implement Service Oriented Architectures and exchange EHR of patients. We give particular emphasis on the reliability of a service-oriented architecture based on the mathematical foundations, which characterize its essential elements, and model how the reliability of the whole application is affected by the system and the EHR growth. When Web healthcare IT chooses the Web Services paradigm, then software and system reliability demands for secure Web Services and proper use of EHRs. The main features that make Web Services attractive, such as accessibility to data, powerful software connections, platform independence and open run-time environments are the threats for sensitive patient information.

In the following section we provide background information related to EHR with respect to information sources that contribute to a patient's EHR and applications that process EHR data in a larger scale (i.e. for many patients) in order to draw useful knowledge. Then we proceed by presenting the needs for security and quality in healthcare and focus on a crucial aspect of healthcare systems' quality, namely the software reliability. For this reason, we present several statistical models that can be used for measuring software reliability and estimating the viability of the Healthcare application.

BACKGROUND ON ELECTRONIC HEALTH RECORDS

A carefully designed Health Information System which includes various fields related to patient care could be used as a tool for extracting statistical information concerning patients' health. The use of information systems for this purpose is a practice that is being studied recently. The Utrecht study (Grobee et. al., 2005) combined the traditional epidemiological studies with the strength of the Electronic Health Record that is being kept in Primary Health Care Facilities. Another study was carried out in 2004 (Majeed, 2004) which