Chapter VIII

Secure Internet Access to Medical Data

Ulrich Ultes-Nitsche
University of Southampton, United Kingdom

Stephanie Teufel
University of Fribourg, Switzerland

INTRODUCTION

In Holbein et al. (1997) and previous papers (Holbein & Teufel, 1995; Holbein et al., 1996), the concept of a context-dependent access control has been introduced and discussed exhaustively. A prototype implementation of the concept is described in Nitsche et al. (1998). The prototype implementation is for local use only and would reveal many security holes if used over an open network: The dynamic link library (DLL) that handles the access control, for instance, would be publicly accessible. In Nitsche et al. (1998), by spying out the DLL code, one could obtain information about the database’s administrator log-in procedure, possibly leaving the entire database unprotected. However, using technology different from that presented in Nitsche et al. (1998) allows one to come up with a secure distributed solution to context-dependent access control over the Internet.

In context-dependent access control, information about the state of a business process is combined with general knowledge about a user to grant or revoke access to sensitive data. The basic concepts of such an access control scheme are understood very well (Holbein, 1996). However, when developing a concrete system one faces several problems: Existing access control mechanisms of the target platform have to be adapted to support context dependency, missing features have to be realized in some indirect way, etc.
It is the aim of the current chapter to present an implementation concept for context-dependent access control on the Internet. Even though applied to the specific application area of clinical trials, the underlying concepts are general and support all applications for which context-dependent access control is suitable. The chapter summarizes a part of the Swiss National Science Foundation funded project MobiMed (Fischer et al., 1995). The system we are going to describe is PC-based (Windows NT) and implemented as a Java servlet accessing an MS SQL Server database. The servlet extends the functionality of Java Web server, which makes it accessible from the Internet. Context information, which is used for checking the authority of an access request, is delivered by an Action Technology workflow system.

This chapter emphasizes the novel technical solution to accessing medical data over the Internet under a context-dependent access control policy. So we concentrate very much on describing the impact that the use of Java servlets has. More aspects of context-dependent access controls can be found in Röhrig and Knorr (2000). After a short introduction into context-dependent access control, we present the basic implementation concepts. To give a detailed description of the implementation of context-dependent access controls, we give an overview of the components that ensure security. Finally, we discuss the appropriateness of the presented solution.

CONTEXT-DEPENDENT ACCESS CONTROL

Role-based security approaches fit well the hierarchically structured setting of a hospital (Ting et al., 1991, 1992). Each level in the hierarchy can be mapped to a so-called organizational role that a person at this hierarchical level plays in the hospital (e.g., medical personnel, care personnel, etc.). After an analysis of each role’s demands on obtaining particular data to perform work, access rights are assigned to each role. The access rights determine which records in the database that contains information about the patients (patient records) may be read or written by a person playing a particular role. When logging in, a user of the system identifies her- or himself by using a chipcard and a PIN, and then a role is assigned to the person according to user/role lists, determining her or his access rights. A different way to handle role assignment is to store role information on the chipcard itself in ciphered form, which then is read during log-in or, alternatively, whenever data records are accessed.

Simple role-based access control mechanisms have the advantage that they can be implemented rather easily but the drawback of certain inflexibilities. A more sophisticated access control technique refining the role-based
Related Content

A Cross-Sectional Evaluation of Illness Perception About Asthma Among Asthma Patients at a Referral Tertiary Care Public Chest Hospital in Delhi, India
[www.igi-global.com/article/cross-sectional-evaluation-illness-perception/70224?camid=4v1a](www.igi-global.com/article/cross-sectional-evaluation-illness-perception/70224?camid=4v1a)

Development of Dual Video Acquisition and Parallel AVI Player with Camera Calibration System for Supporting Dual View Motion Detection
[www.igi-global.com/article/development-dual-video-acquisition-parallel/46059?camid=4v1a](www.igi-global.com/article/development-dual-video-acquisition-parallel/46059?camid=4v1a)

An Advanced and Secure Symbian-Based Mobile Approach for Body Sensor Networks Interaction
[www.igi-global.com/article/advanced-secure-symbian-based-mobile/51618?camid=4v1a](www.igi-global.com/article/advanced-secure-symbian-based-mobile/51618?camid=4v1a)
Introduction
www.igi-global.com/chapter/introduction/23377?camid=4v1a