A Comparative Analysis of Chain-Based Access Control and Role-Based Access Control in the Healthcare Domain

Esraa Omran, Gulf University for Science & Technology, Kuwait City, Kuwait
Tyrone Grandison, Proficiency Labs, Ashland, OR, USA
David Nelson, Faculty of Applied Sciences, University of Sunderland, Sunderland, UK
Albert Bokma, Avedas Information Management, Karlsruhe, Germany

ABSTRACT

The importance of electronic healthcare has caused numerous changes in both substantive and procedural aspects of healthcare processes. These changes have produced new challenges for patient privacy and information secrecy. Traditional privacy policies cannot respond to rapidly increased privacy needs of patients in electronic healthcare. Technically enforceable privacy policies are needed in order to protect patient privacy in modern healthcare with its cross-organizational information sharing and decision making. This paper proposes a personal information flow model that proposes a limited number of acts on this type of information. Ontology-classified chains of these acts can be used instead of the “intended business purposes” in the context of privacy access control. This enables the seamless integration of security and privacy into existing healthcare applications and their supporting infrastructures. In this paper, the authors present their idea of a Chain-Based Access Control (ChBAC) mechanism and provide a comparative analysis of it to Role-Based Access Control (RBAC). The evaluation is grounded in the healthcare domain and examines a range of typical access scenarios and approaches.

Keywords: Access Control, Chains, Healthcare Information Systems, Information Protection, Personal Information Management, Role Based Access Control

INTRODUCTION

Healthcare environments are a complex web of medical professionals and systems (both electronic and non-electronic). As the data being used, stored and transmitted in these environments are valuable and may have several negative outcomes attached to them, the privacy and security of this data is of utmost importance to patients, healthcare staff and the supporting Information Technology (IT) specialists. In this paper, we focus on the fundamental privacy and security mechanisms that are the foundation of healthcare IT systems; with an emphasis on comparing their use in real situations.

DOI: 10.4018/jisp.2013070103
In this paper, we deal with a complex systems scenario from the healthcare domain. Our work is based on work performed at the International Clinic in Kuwait (2011), which is distributed over several locations and serves a patient community in excess of 100,000. Consequently, there are a large number of professionals who are involved in a patient’s care and who need access to patient records. The case is complex for a number of different reasons. There is an evolving set of patients and their records. There are a large number of different types of healthcare professionals, ancillary staff and management staff who deal with patients on a daily basis, and need appropriate access to records to perform their job. Finally there is a need to selectively share information with other healthcare organisations, third party service providers and insurance companies. Health records are particularly complex due to the sensitivity of the records and the need to provide maximum protection (Dick et al., 1997), while allowing access to that data by a large number of users who may require access to specific aspects of the records for varying specific purposes. This field is also heavily regulated; due to the sensitivity of the records and privacy implications. Many countries (University of Alberta, 2005; Webster, 1990) have healthcare-specific data and privacy protection legislation that prescribes the need for record keeping and restricting access to these records for only legitimate purposes.

We contend that this complexity causes several problems, which include:

1. It is difficult for database administrators to correctly define access privileges; giving rise to errors;
2. It is more difficult for another database administrator to subsequently maintain access restrictions;
3. There is an increased opportunity for unintended side-effects when complex privileges are interpreted by the system;
4. Solutions take more steps to compute and cause runtime inefficiencies when privileges have to be checked for a given request.

It would be desirable to have a simpler solution that is easier to configure, maintain and reliably execute. Our proposition is that simple controls and solutions scale and perform better as systems become more complex. This has proven true in other domains, e.g. massively-parallel processing with HADOOP (Borthakur, 2007), and it is hoped that it will be true for security and privacy mechanisms. Currently, the most widely adopted approach to access management, which is supported by the major database systems providers, is Role Based Access Control (RBAC). We purport that RBAC can be complicated to apply in healthcare scenarios and that a simpler approach is needed.

Based on an original concept presented by Al-Fedaghi (2007) we have operationalised the concept of the Chain-Based Access Control (ChBAC) and carried out an evaluation. To this end, we conduct experiments in a complex healthcare environment in order to compare ChBAC with RBAC.

Generally, the application of an effective approach has two phases that must be supported, namely the design phase where the system programmer needs to implement access policies and the runtime phase, where attempts to access data need to be assessed and either be granted or denied. Consequently, any useful method needs to be both easy to apply correctly during the design phase and efficient during runtime. Our evaluation in this paper concentrates on the design phase and we intend to report on the runtime performance in a future publication. Before proceeding with the experiments we will firstly discuss related work, and then outline the Chain-Based Access Control model.

RELATED WORK

We recognize that there are a variety of techniques that have been proposed including: RBAC; Enterprise Privacy Authorization Language (EPAL) (EPAL, 2009); the Platform for Privacy Preferences (P3P) (W3C, 2009); Hippocratic Database (HDB) (Agrawal et al., 2002); and Platform Privacy Preference (P3P) (W3C, 2009). We classify the attempts to preserve
Related Content

Safety and Security in SCADA Systems Must be Improved through Resilience Based Risk Management
www.irma-international.org/chapter/safety-security-scada-systems-must/73129/

Smart Card Applications and Systems: Market Trend and Impact on Other Technological Development
www.irma-international.org/chapter/smart-card-applications-systems/23370/

Policy Enforcement System for Inter-Organizational Data Sharing
www.irma-international.org/article/policy-enforcement-system-inter-organizational/50306/

Assessing Risk and Safeguarding Rare Library Materials During Exhibition Loans
www.irma-international.org/article/assessing-risk-and-safeguarding-rare-library-materials-during-exhibition-loans/148211/

Classifying Articles in Information Ethics and Security
www.irma-international.org/chapter/classifying-articles-information-ethics-security/13454/