A Healthcare Information System with Augmented Access Controls

Nagajyothi Gunti[1], Weiqing Sun[2], Mingzhe Xu[2], Zidong Liu[1], Mohammed Niamat[1], Mansoor Alam[1]

[1]Department of EECS, The University of Toledo, Ohio, USA
{nagajyothi.gunti, zidong.liu, mohammed.niamat, mansoor.alam2}@utoledo.edu
[2]Department of ET, The University of Toledo, Ohio, USA
{weiqing.sun, mingzhe.xu}@utoledo.edu

Abstract. In the healthcare industry, the old paper-based record is becoming a thing of the past and more and more patient information is being transferred into the digital format, that is, Electronic Medical Record (EMR). It integrates heterogeneous information within the Healthcare Information Systems (HIS) stressing the need for augmented security, availability and access controls. We demonstrate our prototype system that incorporates the isolation and delegation components based on the real world HIS software OpenEMR. This system is targeted at enhancing the usability of contemporary HISs without degrading the system security.

1 Introduction

In today's world, technology is constantly changing which reshaped the healthcare and revolutionized the medical profession. The healthcare industry is currently undergoing a gradual migration from the old paper-based patient record system to the Electronic Medical Record (EMR) system. However, protecting the security of these patient records requires a solid infrastructure and a proven security mechanism. Access control is at the heart of the Healthcare Information System (HIS) as it is the key technique to protect and make efficient use of the vast amount of electronically stored medical information. Although traditional Role-based Access Control Model (RBAC) [1, 2] employed by most HISs provides security against unauthorized accesses, it also causes usability issues. For instance, intern doctors during training cannot access the HIS without the supervision of the doctors. And such a strict access control has led to the tragic event [3].

We design our system to accommodate the special access requirements for the medical professionals in HIS which will not be granted as dictated by the traditional RBAC. The rest of the paper is organized as follows. Section 2 provides an overview of our system. Section 3 describes the implementation and evaluation of the system. Finally, we conclude in Section 4.

2 System Overview

We designed our system as shown in Figure 1 by incorporating the access control mechanism based on two models: I-RBAC model [4] and Role-Delegation model [5]. By using the I-RBAC model, the operation on the object by the role is executed inside an isolation environment if the role or operation is predefined to be isolated. This enables the system administrators to specify the roles that need to be first isolated and then checked for security and consistency violations. Such special roles can include new employees, intern doctors and others. In the Role-Delegation model, a junior role can be temporarily granted the senior role's permissions by means of delegation. However, the junior role is not allowed to take the permissions which are only granted to the senior role. This can be especially useful to accommodate emergency or unusual situations in HIS. To make it more secure, after the delegation request is granted, our system will redirect the operations from the delegatee to access the isolated patient records and use the security check to ensure that the operations would not lead to security or consistency violations.

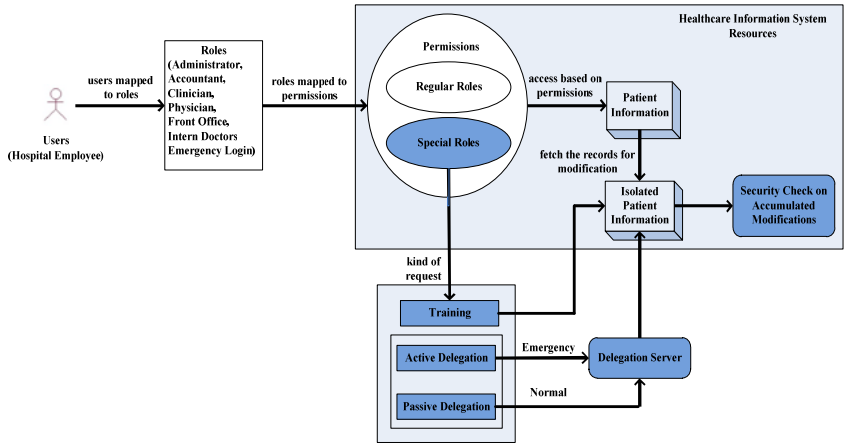

Fig. 1. Augmented Access Controls in Our System

3 System Implementation and Evaluation

Our system was implemented based on OpenEMR. It is a full featured electronic medical record and practice management system which is free, open source, compliant with HIPAA standards and supported on a variety of platforms. The user interface is web based, making the look and feel more familiar to less technical users and more accessible to all users. Some of the features of OpenEMR include management of electronic health records, electronic billing system, support for multiple coding systems, prescriptions, patient statements and reporting. OpenEMR was built upon LAMP (an acronym for Linux, Apache, MySql and Php/Perl/Python) architectural platform. It provides the basic role-based access control, which protects data in the

system from inappropriate accesses. Our system enhances the access control mechanism by incorporating two important components: isolation and delegation. In addition, software modules for the configuration and analysis related with the two components are provided.

3.1 Isolation

Our system provides a dynamic isolation environment for the specified roles to perform their operations inside. Isolation is achieved through dynamically intercepting the database operations by the role and redirecting the operations to the isolated data objects. If there is no isolated data object originally inside the isolation environment, a copy-on-write operation will be invoked to prepare such an isolated copy. This can be implemented at three different levels: database level, table level and record level. We chose the table level approach for the sake of simplicity and reasonable performance and storage overhead. With that, there will be two versions of the same table in our system after the isolated roles modify the table, for instance, *patient_data* table is the original table for storing the patient records, and *ipatient_data* table is its counterpart inside the isolation environment. At the end of the isolated session, a summary log of conflicts or violations will be automatically created by verifying all the isolated operations against the security and consistency policies specified by the system administrators.

We provided an isolation administration web page as shown in Figure 2. This page is visible only to the administrator. And the administrator can add/remove isolated roles and specify isolated users. He can also view the log information of each isolated user from the log column.

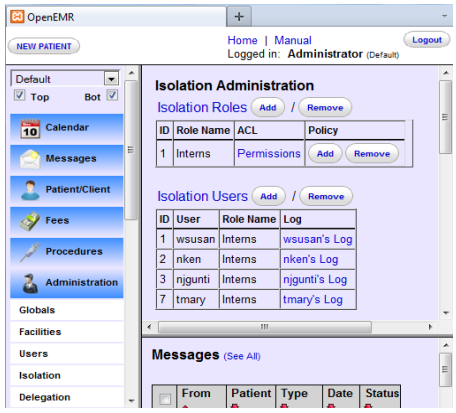

Fig. 2. Isolation Administration

3.2 Delegation

The delegation component is implemented by developing a delegation server which decides to grant the delegation requests based on certain rules. There are two delegation modes, active delegation and passive delegation, which are used for emergency situations and normal cases, respectively. One unique feature of our system is that isolation is used to support the delegation service. Even if the delegation request is granted, the system can isolate the operations of the delegatee, and then verify the net-effect of the isolated operations before applying them to the original system. This provides another level of protection because it is possible that the delegatee could

commit unexpected errors. In addition, the administrator has a delegation administration web page to manage delegation related functionalities.

We evaluated our system by defining the intern doctors as the special role to be isolated. Instead of being denied any access to the system, the intern doctors could access the system inside an isolation environment during the training phase. They could also request the active delegation under emergency situations. The accumulated isolated operations would be automatically verified against the security/consistency policies after the session of the intern doctors and the violations would be reported to the system administrators.

4 Conclusions and Future Work

Our system can grant the needed accesses to medical professionals, such as intern doctors, in a secure and controlled manner. Those accesses would be otherwise denied in HISs with traditional access control models. In our system, the isolation and delegation services can be configured to support access requests from certain special roles (or users). For the future work, we plan to realize the isolation environment in a more efficient way by implementing copy-on-write and redirection operations at the record level. We will also enhance the delegation service by incorporating the trustworthiness and capability values of the delegation candidates. In addition, we plan to invite medical professionals to use and evaluate our system, and their feedback will be analyzed and used to further improve our system.

References

1. D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn and R. Chandramouli, Proposed NIST standard for role-based access control, *ACM Trans. on Information and System Security (TISSEC)*, pp. 224-274, Aug. 2001
2. R. S. Sandhu, E. J. Coyne and H. L. Feinstein, C. E. Youman, Role-Based Access Control Models, in *Proc. IEEE Computer Security*, vol. 29, no.2, pp. 38-47, Feb. 1996

3 C. J. Duh, *EMR's Will Save Time and Improve Coordination.* Retrieved August 22, 2011. From Doctors for America: http://www.drsforamerica.org/blog/emr-s-will-save-time-and-improve-coordination

4. N. Gunti, W. Sun and M. Niamat, I-RBAC: Isolation Enabled Role-Based Access Control, in *9th Annual Conference on Privacy, Security and Trust*, (Quebec, Canada, 2011), IEEE Computer Security Press, 79-86
5. S. Na and S. Cheon, Role Delegation in Role-Based Access Control, in *5th ACM Workshop on Role-based access control*, (Berlin, Germany, 2000), ACM Press, 39-44