Security Middleware Infrastructure for DICOM Images in Health Information Systems

Vijay N. V. Kallepalli, M.Sc.,¹ Sylvanus A. Ehikioya, Ph.D.,¹ Sergio Camorlinga, M.Sc.,²
and Jose A. Rueda, Ph.D.,³

In health care, it is mandatory to maintain the privacy and confidentiality of medical data. To achieve this, a fine-grained access control and an access log for accessing medical images are two important aspects that need to be considered in health care systems. Fine-grained access control provides access to medical data only to authorized persons based on priority, location, and content. A log captures each attempt to access medical data. This article describes an overall middleware infrastructure required for secure access to Digital Imaging and Communication in Medicine (DICOM) images, with an emphasis on access control and log maintenance. We introduce a hybrid access control model that combines the properties of two existing models. A trust relationship between hospitals is used to make the hybrid access control model scalable across hospitals. We also discuss events that have to be logged and where the log has to be maintained. A prototype of security middleware infrastructure is implemented.

KEY WORDS: DICOM, security, infrastructure, access control, policy management, log maintenance, health care, middleware, privacy, confidentiality, PHIA

WITH THE INCREASING use of information technology in health care today, picture archiving and communication systems (PACS) in different hospitals are interconnected to share medical images, thereby providing a distributed environment for storing and accessing medical images. As medical images are accessed from various locations in such distributed environments, security becomes a major concern. Security lapses such as unauthorized access, eavesdropping, masquerading, intrusion, and data integrity violation could easily occur. Medical data is highly sensitive, so countries like the United States, Canada, and others around the world have defined policies and introduced

laws to maintain the privacy and confidentiality of medical data.

The Canadian provincial government of Manitoba introduced the Personal Health Information Act (PHIA),¹ which is similar to the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Some of the policies include³¹: (a) A trustee (i.e., a hospital, walk-in clinic, etc.) should provide each of its employees access only to medical information for which he/she is designated. (b) A trustee should maintain a log of every successful and unsuccessful attempt to access health information, and perform regular audit to detect security breaches, (c) A trustee can disclose information to another trustee only with the consent of the individual (i.e., patient). (d) A trustee, while transmitting medical data, should take appropriate measures to protect the data from eavesdropping and masquerading, and perform integrity checks.

¹From the Department of Computer Science, University of Manitoba, 561 Machray Hall, Winnipeg, Manitoba, R3T 2N2, Canada.

²From the Department of Radiology, St. Boniface General Hospital Research Centre and University of Manitoba, 351 Tache Avenue, Room 2019-5, Winnipeg, Manitoba, R2H 2A6, Canada.

³From the TRILabs, 100-135, Innovation Drive, Winnipeg, Manitoba, R3T 6A8, Canada.

Correspondence to: Vijay N. V. Kallepalli, M.Sc., St. Boniface General Hospital Research Centre, 351 Tache Avenue, Room 2019-5, Winnipeg, Manitoba, R2H 2A6, Canada; tel: 204-235-3584; fax: 204-231-1164; e-mail: Vijay@cs.umanitoba.ca

Copyright © 2004 by SCAR (Society for Computer Applications in Radiology)

Online publication 30 January 2004

doi: 10.1007/s10278-003-1710-7

The hospitals in the Canadian city of Winnipeg are being interconnected to share medical data in a distributed environment. The users' roles and object access domains change dynamically based on time, location, content, and priority. The process of providing fine-grained access control is further complicated when access control has to be scalable across hospitals. The complexity deepens because we are dealing not only with users known to the trustee but also with users unknown to the trustee. Therefore, protecting and providing fine-grained access control to digital imaging and communication in medicine (DICOM) images based on PHIA is one of the major challenges in PACS.² Traditionally, access control is provided with techniques such as Discretionary Access Control (DAC),³ and Mandatory Access Control (MAC).⁴ In DAC the access is provided based on owner's discretion (i.e., a user responsible for the creation of data grants/denies access to the data by another user). In MAC, the security administrator sets up rules for data access, and the user has to satisfy those rules to gain authorization to access data. Both MAC and DAC have lost their importance with the introduction of Role-Based Access Control (RBAC).⁵ In the RBAC model, a user activates his/her permissions by selecting a subset of assigned roles (i.e., a job or a task performed in an organization), which in turn are associated with a set of permissions. RBAC provides flexibility and centralized security administration, reduces security administration overheads, and follows a normal workflow in an organization. The RBAC model eliminates the need to define the rights for each user with respect to the objects that he/she is authorized to access; instead, roles are defined and assigned to users. The RBAC model is a passive security model, as it does not take context into consideration.

The RBAC model as such cannot be used in Information Systems in the Radiology Department (ISRD) because it provides access control at the object level but not at the instance level. In this context, *object* refers to patients' medical records and *instance* refers to a specific patient's medical data. In an ISRD, physicians have access only to their own patients' medical data. Chandramouli⁶ proposes a framework—Dynamic Authorization Framework for Multiple

Authorization Types (DAFMAT)—that provides a hybrid access control model and a logic-driven authorization engine. The hybrid access control model combines the properties of RBAC and domain type enforcement. DAFMAT provides access control dynamically but it is complex to build, degrades the performance of an ISRD, and provides access only within a single hospital.

Recent trends gravitate toward active security that provides access based on time, location, content, and priority. Team-based Access Control (TMAC)⁷ is an example of an active security model. TMAC is an extension of RBAC with an additional component called a “team.” In TMAC, a team represents a set of health care professionals providing treatment to a given patient. The access rights of the members of the team are determined according to their roles within the organization. Unlike the RBAC model that provides access control at an object level, TMAC provides access control at an instance level. TMAC as such cannot be used to provide access control across hospitals because the external users (i.e., user in another hospital) are not recognized locally.

Zhang et al⁸ propose a framework that supports role-based delegation based on rules, the Rule-Based Role Delegation Model (RBRDM). This framework allows a user to delegate some of his/her roles to another user. Although RBRDM can be extended to support health care information systems, delegation alone will not fulfill the requirements of access control in the health care domain. For instance, a general practitioner lower in the medical role hierarchy has a requirement to refer a patient to a specialist higher in the role hierarchy. This scenario, which is quite common in the health care domain, is not permissible with RBRDM. RBRDM allows only persons higher in the hierarchy to delegate some of his/her roles to a person lower or equal level in the role hierarchy. In RBRDM, roles are delegated only for a specific period of time, after which delegated roles are revoked, even if the task has not been accomplished. In a scenario such as the one discussed before and when a physician in another hospital is referred, it is difficult to determine the delegation time. Zhang et al⁸ argue that “team” in TMAC is an additional

constraint that can be checked at run time. But without teams it is difficult to determine if a user is responsible for treatment of a particular patient, especially when access control has to be provided across hospitals and will therefore involve external users. RBRDM reduces security administration overheads considerably. Our work is closely related to both TMAC and RBRDM because we combine these two models and use the trust relationship between hospitals to make access control scalable across hospitals.

We can build a secure information system by providing authentication, authorization (i.e., access control), cryptography, and many other components. Authentication validates the identity of the user, while authorization determines which user can access which objects in an organization (i.e., it defines the access rights the user possess in an organization). However, no system in this world is perfectly secure. We need mechanisms to detect and analyze security breaches in information systems. If a user of an information system performs an action that he/she is not legally allowed to perform, it is known as *intrusion*. Intrusion may happen internally or externally to the hospital network. A detection mechanism identifies unauthorized access and notifies the security administrator of potential intrusions based on logged data analysis (here logged data represents the events occurring in the network), and configures itself to avoid intrusions. Intrusion detection is a three-step process: collecting log data, analyzing logged data, and countering intrusions. Log data collection and log data maintenance are important aspects of intrusion detection mechanisms. In the health care domain, it is important to determine who violated the rules set by provincial or federal governments and thereby safeguard the privacy and confidentiality of the medical data.

To avoid violation of the access rules, audit data must be collected at the application level, in addition to the audit data collected at system level. Syslog,⁹ a UNIX utility tool, is proposed for collecting audit data in a distributed environment. However, syslog reports only failures to audit repositories at the system level. According to PHIA,¹ a log has to be maintained not only for failures but also for successful attempts to access medical data. This requirement

is necessary because violations may occur even in successful attempts. It is also important to capture events at the application level, to determine who provided a user the authority to access a particular patient's data, etc. This feature is unavailable in the application of the syslog in an integrated health enterprise. In contrast to syslog application, our log maintains both successful and unsuccessful attempts to access medical data, as well as events that occur at the application level. Axelsson¹⁰ presents an in-depth survey of intrusion-detection systems. This survey indicates that there is little information about what data should be captured for a security log. The scope of this article is to discuss events at the application level that need to be logged and where the log data has to be maintained.

The DICOM standard¹¹ provides mechanisms for application entities to perform integrity checks, secure authentication, and secure transfer of data between application entities, thereby providing solutions to eavesdropping, wire-tapping, and masquerading. But DICOM does not provide any standard mechanism to support access control, log maintenance, and policy management.

In this article we describe a security middleware for DICOM images that provides fine-grained access control, policy management, demographics filtering, and log maintenance constrained to the Canadian-Manitoban PHIA and the DICOM standard. Our emphasis is on fine-grained access control and log maintenance. The security infrastructure that we provide maintains the privacy and confidentiality of DICOM images, without significantly degrading performance, while increasing scalability and fault-tolerance in an enterprise set of hospitals. We discuss the hospital's trust relationship in the Methods section.

METHODS

As shown in Figure 1, the major components of our security middleware are authentication, authorization, policy management, filtering, and log maintenance engines. Our security middleware also includes standard mechanisms provided by DICOM standard Work Group-14 for authentication (user name and password, KERBEROS, biometrics), an integrity check (public-key infrastructure), and secure communication (transport layer security, secure

Fig 1. Architecture of security middleware infrastructure.

Fig 2. Security nodes depending on the size of the hospital network.

socket layer). In a hospital network, our security middleware acts as a gateway (security node) between clients (reading work stations and modalities) and data-storage repositories. We assume that each gateway has a patient location system that identifies the location of patient's DICOM images present at various storage repositories in the hospital network. Furthermore, depending on the size of the hospital network, each hospital should have at least one security node (Fig 2). We also assume that the security nodes across hospitals trust each other and share patient medical information expeditiously. Walk-in clinics, laboratories, and research centers that cannot afford the middleware can be come affiliated with one of the security nodes located in the nearest hospital (Fig 3). We discuss the functionality of the components of the security middleware below.

Access Control

The authorization engine performs authorization checks (i.e., access control) in a hospital. We provide the access control by combining TMAC and RBRDM. In a hospital, a "team" (consisting of primary physician, nurse, and resident medical student) is formed around a patient. The members of the team are responsible for that patient's treatment. The access permissions of the members of the team are determined based on their assigned roles in the hospital. Each role is assigned a set of services, and these, in turn, are assigned a set of DICOM standard operations. We maintain two separate teams for each patient: an "assignment team" and a "delegation team." The assignment team is created when the patient arrives at the hospital. The members of the patient's assignment team can further assign or delegate other users to their patient's team to access the patient's

Fig 3. Hospital network.

medical data. The members of the delegation team, cannot themselves perform assignment and delegation operations.

The roles in the hospital are arranged in a hierarchical order and rules for assignment, delegation, and revocation are defined for the roles. Roles higher in the hierarchy inherit properties from the roles below them. This property of RBRDM reduces the security administration overhead by eliminating the need to define rules for each and every role. As shown in Figure 4, a user presents his/her credentials to the authentication engine. Then the authentication engine performs the validation of the user and returns a set of roles he/she is assigned in the hospital. The user is prompted to select one of the assigned roles and tries to access a service on patient's data. The authorization engine, based on the role selected and the service requested by the user, checks whether the user belongs to the patient's team and determines the authorization of the user. The security node processes the request if the patient's data are directly under its control; otherwise the request is dispatched to the security node (internal or external to the hospital network) containing the patient's data in an XML (extensible markup language) file. The security node (internal or external to the hospital) trusts authentication performed by another security node.

Fig 4. Access control.

Trust in ISRD

We define trust in ISRD as the belief or confidence that a trustee places in another trustee in maintaining the privacy and confidentiality of medical data. Each trustee has at least one security node that contains the security middleware. An approval committee determines the trustworthiness of a security node. Upon approval, the security node is known as a “registered security node” and the registered security node’s information is broadcast to every security node in the hospital network. When requested medical data are unavailable directly in a registered security node, a request on behalf of a client is made to another registered security node where the requested patient’s medical data exist. The registered security node can use a patient location service to find the patient’s medical data. The patient location service contains meta-data information such as patient identification and the location (i.e., network address of the registered security node) where the data is available. The registered security nodes at different hospitals in the network communicate with one another through an agreed trusted port, using a special public key. If the request originates from a registered security node through a trusted port, the registered security nodes process the request without any further authorization checks. The requesting registered security node acts as a mediator between the client and the original registered node processing the request. Therefore, the authentication and authorization checks are performed locally, but access to medical data is provided globally.

Policy Management

Policies are arranged in a systematic order in a database. In Canada, each province has many hospitals, and each hospital has four categories of policies: assignment policies, delegation policies, revocation policies, and access policies. Assignment and delegation policies are the rules that define which users in a particular role can assign or delegate some of their responsibilities to specific users in another role within an organization. Revocation policies are the rules that determine the users in a particular role that can revoke the granted rights from specific users in another role in an organization. Access policies determine the services the

users in a particular role can access in an organization. The security administrator defines the policies for a hospital, and the policy management engine manages the policies of the system and fires appropriate rules based on the operations performed by the user at run-time.

Filtering Demographics

The filtering engine is used to filter demographics (such as patient name, age, gender etc.) embedded in the DICOM medical images while disclosing information to researchers. A DICOM file is a set of data elements. Each data set contains a tag, value representation, value length, and value field. The filtering engine identifies the tags representing the demographics while parsing the DICOM file. The filtering engine replaces the identified demographic values with some delimiter. Figure 5, shows a sample DICOM file before and after filtering the demographics. However, the information requested has to be approved by a research approval committee prior to disclosure.

Log Maintenance

The access log can be maintained in one of three locations: the location from which the request originated, the location at which the request is processed, or a centralized location for a group of hospitals within a region. The log maintenance engine keeps track of user information, operation performed, access location, time-stamp, and access policy. We maintain three separate logs: an authentication log, an access log, and an assignment, delegation, and revocation log. The authentication log records the user name, network address of the machine from which the request originated, timestamp, and result. The result can be either successful or unsuccessful. The authentication log can be centralized within the hospital or distributed. In a decentralized system, the authentication log is maintained at the location where the request is processed. The access log records the user name, the user’s role in the organization, the name of the organization where the request originated, the DICOM service requested, the network address from where the request originates, timestamp, patient name, and the result, which can be either successful or unsuccessful. An

Fig 5. Filtered DICOM file sample.

Fig 6. Conceptual view of security middleware infrastructure.

access transaction is recorded at the location closest to where the request is processed. An assignment, delegation, and revocation log record the user1 [i.e., assigning, delegating, or revoking user], user1 organization, user2 [i.e., assigned, delegated, or revoked user], user2 organization, operation performed (i.e., assignment, delegation or revocation operation) patient name, timestamp, and result. The access log aids in the investigation of any security breaches. PHIA states that audits must be performed at regular intervals, but manual auditing is a cumbersome process because of the vast amount of data involved. We assume the existence of auditing mechanisms to detect security breaches automatically.

Data Integrity

The conceptual view of the security middleware to access DICOM images is shown in Figure 6. We use secure socket layer (SSL) between clients and the security nodes (internal and external to the hospital network) to ensure data integrity and protect data from eavesdropping. As shown in Figure 2, access can be controlled either through a single security node (centralized architecture; see Hospital 3, Fig 2) or multiple security nodes (decentralized architecture; see Hospital 1, Hospital 2, and Hospital 4, Fig 2). Centralized access control provides better access control, but it may lead to bottlenecks (i.e., if the single security node fails, the data under it cannot be accessed until it is rectified) and may degrade in performance as the load increases. The fault-tolerance level is quite low because there is a single point of failure. The decentralized model resolves the problems associated with the centralized model, but it may lead to inconsistencies whenever an entity is added or deleted from the access control lists or the policy lists, and to overloading a single security node

out of multiple security nodes. In our prototype implementation, we maintained and accessed the user information, team information, policies, and patient information in a centralized database within a hospital network. However, in real-time implementations we can avoid the problems of inconsistency and overload by applying appropriate replication techniques to maintain the consistency among the replicated data and use load-balancing technique to distribute the load.

RESULTS

We make the following assumptions to discuss the case studies.

1. Three hospitals A, B, and C are interconnected either by a dedicated network or a virtual private network.
2. Each of the hospitals has an ISRD, such as PACS/radiology information system (RIS)/health information system (HIS), to access DICOM medical images and at least one security node.
3. The number of security nodes in a hospital depends on the size of the hospital network.
4. An approval committee approves the researcher's requests.
5. The RIS/HIS generate an event when a user completes a job or when a patient leaves the hospital. The events are propagated to the security nodes, where an assignment operation is performed.

6. The approval committee approves the registration of a security node. The registration event should be propagated to each and every security node in the network.
7. The RIS/HIS supports a Master Patient Index (MPI) that identifies a patient uniquely in the network.
8. The RIS/HIS supports a patient location system that locates the patient's data in the interconnected hospital network based on the unique identifier obtained from the MPI.

Case Study 1: A Patient Visits a Hospital for Treatment

Let us assume Sam, a patient, visits hospital A. Catherine, a receptionist at the hospital's front desk, registers Sam, after which he goes for preliminary analysis. Catherine assigns Jennifer, the staff person responsible for preliminary analysis, to Sam's assignment team. Jennifer performs the preliminary check up and generates a report. The ISRD generates an event when Jennifer submits the report, and that event deletes Jennifer from Sam's assignment team. When Catherine receives the report, she assigns Dr. John to Sam's assignment team; the choice of physician is based both on the preliminary analysis report and availability of medical staff. Dr. John's access rights are determined based on his role in the organization. He can further assign or delegate another user to access Sam's radiology data. The members of Sam's assignment team actively participate in the team management; therefore, our model is an active security model. The members of Sam's assignment team change dynamically based on the requirements.

Case Study 2: A User Assigns Another User to a Patient's Team Within a Hospital

Dr. John, the only active member of Sam's assignment team, makes a diagnosis and refers Sam to Dr. Smith, a cardiologist in the hospital A. Access control checks to see if Dr. John is authorized to assign Dr. Smith to Sam's team. The assignment of Dr. Smith to the team is based on the assignment rules and constrained

to the fact that Dr. John is himself a member of Sam's team. If permitted, Dr. Smith is added to the team and permissions are granted to Dr. Smith to access Sam's radiology data. Dr. Smith is granted that access only if he remains on the team. Drs. John and Smith, both members of Sam's team can further assign other users in hospital A, based on assignment rules and requirements.

Case Study 3: A User Assigns Another User to a Patient Team Outside a Hospital

Consider a scenario in which Dr. John in hospital A wants to assign Dr. Ram in hospital B and Dr. James in hospital C to Sam's assignment team. The security node based on the assignment rule processes Dr. John's request. If permitted, Dr. John's request is dispatched to the security nodes in hospital B and hospital C in XML format; otherwise the request is denied. The security nodes in hospital B and hospital C add Dr. Ram and Dr. James to Sam's assignment team at hospital B and hospital C, respectively. Now Drs. Ram and James can access Sam's medical data based on their roles in their respective organizations. The size of assignment teams in hospital B and hospital C may grow at the discretion of Dr. Ram and Dr. James. We assume that users on the assignment teams access their assignment and delegation rights legally and only as needed. However, a log is maintained and auditing is performed at regular intervals to detect any illegal operations. The users Dr. Ram and Dr. James are excluded from Sam's assignment team either at the completion of the task or at the generation of an event from the node at which the assignment operation originated. The users assigned and delegated to access Sam's radiology data are excluded recursively from assignment and delegation teams upon receipt of the event generated by the RIS/HIS.

Case Study 4: A User Delegates and Revokes Rights of Another User to Access Patient's Medical Data

Dr. John, a member of Sam's assignment team, finds himself busy and wants his subor-

dinates to provide care temporarily. Dr. John adds Jack (i.e., a resident medical student) to Sam's delegation team to give Jack temporary access to Sam's radiology data. Jack accesses Sam's radiology data based on the services available to the resident medical student role in the organization. However, Dr. John, based on the requirements of the case, may delegate a subset of the services he possesses to Jack, enabling Jack to access Sam's medical data. The access rights are revoked either at the end of expiration time or at the discretion of Dr. John. However, the delegation and revocation of rights is permitted based on the available delegation and revocation rules.

Case Study 5: A User Accesses DICOM Services on Patient's Medical Data

The members of Sam's assignment or delegation teams can access DICOM services on Sam's radiology data. The security node, transparent to the user, performs the necessary authorization checks. The authorization check is constrained in that the user must be a member of the Sam's assignment or delegation team and the DICOM service requested must be on the list of DICOM services for the role the user possesses in the organization. For instance, Dr. John, acting as a general practitioner in hospital A, asks to retrieve Sam's radiology data. Because the DICOM service is available to general physicians in hospital A, Dr. John can retrieve patient's medical data. Because Dr. John is a member of Sam's assignment team and possesses the right to access DICOM service (i.e., to retrieve radiology data), the security node at hospital A, by using the patient location service, finds that Sam's radiology data is located at hospital B and hospital C. After locating the data, the security node at hospital A dispatches the request to one of the security nodes in hospital B and hospital C. The security nodes at hospital B and hospital C trust the security node at hospital A. Therefore, the security nodes at hospitals B and C transfer Sam's radiology data to the security node at hospital A expeditiously. The security node at hospital "A" in turn transfers the radiology data obtained from security nodes at hospitals B and C and the data in its own control to Dr. John.

Case Study 6: Completion of Patient's Treatment in a Hospital

An event is generated by RIS/HIS when a patient's treatment ends. That event removes each member of that patient's assignment and delegation teams recursively until both the assignment and the delegation classifications are empty. In the case of our example patient, Sam, the event is propagated to security nodes at hospitals B and C, where DR. Ram and Dr. James are members of the Sam's assignment team. The propagated event excludes the members of the assignment and delegation teams recursively. This process continues until the chain (of assignment and delegation events) ends.

DISCUSSION

We implemented a prototype of security middleware infrastructure for DICOM images. The middleware provides flexibility (i.e., new security components can be added or removed without modifying the existing application) and lessens the burden on the application developer to include security features in applications. The hybrid access control model (i.e., a combination of TMAC and RBRDM), along with the trust relationship between hospitals, is more flexible, scalable, and reduces the level of security administration required by existing models. Unlike TMAC, which maintains a single team for each patient, the hybrid access control model maintains two teams, an assignment team and a delegation team. With separate teams, it is easy to identify who can further assign or delegate responsibilities to another user in a hospital. Team separation allows better team management. The hybrid access control model also overcomes the problems in RBRDM discussed in the opening paragraphs of this article, such as delegating responsibilities to a user higher in the hierarchy and determining if an external user is responsible for the patient's care. The RBRDM model assumes a static role hierarchy within a hospital and the role hierarchy seldom changes. However, in reality, roles may be added, removed, or modified in the hierarchy. Such changes could lead to security inconsistencies if not done properly. We maintain the

role hierarchy for the hospital in an XML file and have implemented a module that conveys any changes in the hierarchy to the XML file. Therefore, even if the security node crashes the updated role hierarchy is initiated from the XML file. The hybrid access control model uses the inheritance property of RBRDM,¹⁰ thereby reducing the security administration overhead considerably. The trust relationship between hospitals increases the scalability of the hybrid access control model. Because of the existence of a trust relationship, the hybrid access control model performs the authorization check locally and allows the users to access medical data globally. The hybrid access control model is also flexible because it incorporates RBAC,⁴ which allows a security administrator to add or remove roles at any time. In addition, roles can be assigned to or revoked from each user dynamically. The location and content of the log is customized to meet health care needs. All generated logs (e.g., DICOM access service log) aid in the investigation of security breaches.

CONCLUSIONS

In this article, we identified security components and provided a security middleware infrastructure that serves to integrate them. These components allow sharing radiology data securely in a distributed environment across hospitals, walk-in clinics, and research organizations. We implemented a prototype of the security middleware infrastructure for DICOM images. In our prototype implementation, the authentication engine performs user validation, the authorization engine provides access control, the log maintenance engine maintains the log, and the filtering engine replaces the demographics embedded in DICOM images with dummy values. The hybrid access control model constrained to PHIA allows only authorized persons to access DICOM images based on priority (either emergency or ordinary), location, and content. The hybrid access control model performs authorization checks locally while providing access to DICOM images located at different hospitals, thereby increasing the scalability factor of the model. The generated logs can be used in the investigation of security breaches. We use secure socket layer

(SSL) for communication between the client and the security nodes to protect data from eavesdropping and to ensure data integrity. The security middleware infrastructure we provide may be used by health care organizations as a blueprint for sharing radiology data in a distributed environment.

ACKNOWLEDGMENTS

This research project is in collaboration between TR Labs (Winnipeg) and St. Boniface General Hospital Research Center (SBRC). We are grateful to TR Labs and SBRC for funding the project.

REFERENCES

1. The Personal Health Information Act, Regulation 245/97. The Manitoba Gazette Vol. 126 (50), December (1997). (URL: <http://www.gov.mb.ca/health/phia/>).
2. Vazquez-Naya, JM, Loureiro, JP, Dorado, J de la Calle, et al: Necessary security mechanism in a PACS DICOM access system with Web technology. J Digit Imaging. (Special Issue on Inconsistency Management, Society of Computer Applications in Radiology) 15:107-111, 2002
3. A Guide to Understanding Discretionary Access Control. National Computer Security Center, NCSC-TG-01, Version-01, Fort George G. Meade, MD, June 1998
4. Lee TMP: Using mandatory integrity to enforce commercial security. Proceedings of IEEE Computer Society Symposium on Security and Privacy (Oakland, CA), May 1998, pp. 140-146
5. Ferraiolo D, Kuhn R: Role-based access control. proceedings of 15th NIST-NCSC National Computer Security Conference (Baltimore, MD), October 1992
6. Chandramouli R: A framework for multiple authorization types in healthcare application systems. Proceedings of 17th Annual Computer Security Applications Conference (New Orleans, LA), December 2001
7. Thomas RK: Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments. Proceedings of the 2nd ACM Workshop on Role-based Access Control (RBAC'97) (Fairfax, VA), November 1997, pp. 13-19
8. Zhang L, Ahn GJ, Chu BT: A role-based delegation framework for health care information system. Proceedings of 7th ACM Symposium on Access Control Models and Technologies (SACMAT'02) (Monterey, CA), June 2002
9. Reliable delivery for syslog. RFC 3195, November 2001. (URL: <http://www.faqs.org/rfcs/rfc3195.html>)
10. Axelsson S: Intrusion detection systems: a survey and taxonomy. Technical Report 99-15, Department of Computer Engineering, Chalmers University of Technology, SE-41296 Göteborg, Sweden, March 2000
11. Digital Imaging and Communications in Medicine Standard, Security Profiles. Rosslyn, VA: National Electrical Manufacturers Association, 2002