Common Object Request Broker Architecture (CORBA)-Based Security Services for the Virtual Radiology Environment

Ralph Martinez, Colin Cole, Jerzy Rozenblit, Jay F. Cook, and Anna K. Chacko

The US Army Great Plains Regional Medical Command (GPRMC) has a requirement to conform to Department of Defense (DoD) and Army security policies for the Virtual Radiology Environment (VRE) Project. Within the DoD, security policy is defined as the set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. Security policy in the DoD is described by the Trusted Computer System Evaluation Criteria (TCSEC), Army Regulation (AR) 380-19, Defense Information Infrastructure Common Operating Environment (DII COE), Military Health Services System Automated Information Systems Security Policy Manual, and National Computer Security Center-TG-005, "Trusted Network Interpretation." These documents were used to develop a security policy that defines information protection requirements that are made with respect to those laws, rules, and practices that are required to protect the information stored and processed in the VRE Project. The goal of the security policy is to provide for a C2-level of information protection while also satisfying the functional needs of the GPRMC's user community. This report summarizes the security policy for the VRE and defines the CORBA security services that satisfy the policy. In the VRE, the information to be protected is embedded into three major information components: (1) Patient information consists of Digital Imaging and Communications in Medicine (DICOM)-formatted fields. The patient information resides in the digital imaging network picture archiving and communication system (DIN-PACS) networks in the database archive systems and includes (a) patient demographics; (b) patient images from x-ray, computed tomography (CT), magnetic resonance imaging (MRI), and ultrasound (US); and (c) prior patient images and related patient history. (2) Meta-Manager information to be protected consists of several data objects. This information is distributed to the Meta-Manager nodes and includes (a) radiologist schedules; (b) modality worklists; (c) routed case information; (d) DIN-PACS and Composite Health Care system (CHCS) messages, and Meta-Manager administrative and security information; and (e) patient case information. (3) Access control and communications security is required in the VRE to control who uses the VRE and Meta-Manager facilities and to secure the messages between VRE components. The CORBA Security Service Specification version 1.5 is designed to allow up to TCSEC's B2-level security for distributed objects. The CORBA Security Service Specification defines the functionality of several security features: identification and authentication, authorization and access control, security auditing, communication security, nonrepudiation, and security administration. This report describes the enhanced security features for the VRE and their implementation using commercial CORBA Security Service software products.

THE GREAT PLAINS regional medical command (GPRMC) has always been a leader in the development and deployment of new technology into picture archiving and communication systems (PACS). The Brooke Army Medical Center (BAMC) at Ft Sam Houston, TX has the only 100% filmless radiology department in the Army. With the rapid advances in telecommunications, middleware protocols, multimedia network technology, and the requirement to improve health care in the Department of Defense (DoD), the GPRMC has developed the next-generation virtual radiology environment (VRE) for the Army. The purpose of the VRE Project in the GPRMC is to provide a seamless and virtual radiology department among 10 hospital sites initially. The VRE Project is in progress to interconnect major US Army medical centers to medical treatment facilities (MTFs) using a private Army communications network, called MedNet. The VRE Project will provide radiology services to address the issues of cost, improved quality, and medical access in the US Army. The GPRMC has sponsored the development of a hierarchical intelligent controller, called the Meta-Manager, that will manage the VRE operations and control functions. The Meta-Manager specifications and prototype have been developed by the Computer Engineering Research Laboratory (CERL) at the University of Arizona. This report addresses the advanced features of the Meta-Manager and the VRE system that require research and development efforts by the CERL.

The initial phase is a Teleradiology Pilot Testbed consisting of 10 hospital sites in the GPRMC.

From the Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ; and Department of Radiology, Brooke Army Medical Center, San Antonio, TX.

Address reprint requests to Ralph Martinez, PhD, Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ 85721. E-mail: martinez@ece.arizona.edu.

0897-1889/00/1302-1014$10.00/0
doi:10.1053/jdim.2000.6828

BAMC will be the major center for reading and diagnosis of radiology modality cases from the other MTF sites. The VRE Project testbed MTF sites are located at Ft Riley, KS (installed), Ft Hood, TX (spring 2000), Ft Leonard Wood, MO (summer 2000), Ft Huachuca, AZ (March 2000), Ft Polk, LA (spring 2000), Ft Leavenworth, KS (installed), Ft Sam Houston, TX (installed), Ft Carson, CO (fall 2000), Ft Bliss, TX (summer 2000), and Ft Sill, OK (fall 2000). IBM Medical Systems Division (Denver, CO) is installing digital imaging networks picture archiving and commnication system (DIN-PACS) networks at hospitals in Ft Hood, TX, and Ft Huachuca, AZ at the time of writing of this proposal.

In the VRE, patient cases are acquired at the MTF sites and then stored and forwarded to BAMC for primary interpretation readings. The report findings are then returned to the originating MTF site. The VRE Pilot Testbed will serve to evaluate the new IBM PowerPACS products and collect statistics that can be used for the long-term design and implementation of future VRE sites. The cases will be read at BAMC on the PACS workstations by BAMC radiologists. The Meta-Manager will alter the foregoing BAMC-centric routing of patient cases in the VRE system by using intelligent management and control algorithms. The current Meta-Manager will be enhanced to include new features that make the VRE system more robust and reliable. The VRE network and the Meta-Manager system will serve as a model for other DoD and industry developments in teleradiology environments.

The CERL at the University of Arizona has performed research and development for the development and specification of the Meta-Manager. Final versions of the Meta-Manager specifications and deliverables were delivered to the GPRMC in June 1999. The CERL participated in the system design of the VRE Security Policy, modeling and simulation of the VRE communications networks, and the Meta-Manager system. The CERL has also developed a framework middleware for distributed computing environments (DCE) based on the Common Object Request Broker Architecture (CORBA) standards developed by the Object Management Group. The CORBA-based framework allows the implementation of object-oriented applications over a heterogeneous internet working environment. CORBA components include an Object Request Broker (ORB) that is used to discover object resources in an Intranet and associate them with a client. These developments form a starting point for this project.

The security policy and system in the VRE must be compliant with DoD and Army regulations and policy. Within the Department of the Army (DA), security policy is defined as the set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information, such as the DoD Trusted Computer System Evaluation Criteria (TCSEC), Army Regulation (AR) 380-19, and Defense Information Infrastructure Common Operating Environment (DII COE). The VRE security policy defines information protection requirements that are made with respect to those laws, rules, and practices that are required to protect the information stored and processed in the VRE. This report describes the requirement policy for the overall VRE system, DIN-PACS networks, and the Meta-Manager system and describes the use of the CORBA Security Service to satisfy the policy.

The VRE System consists of major components including the DIN-PACS hospital networks, the VRE communications network, or virtual private network, and the Meta-Manager. In the VRE, the information to be protected is embedded in these three major information components:

- Patient information consists of Digital Imaging and Communications in Medicine (DICOM)-formatted fields. The patient information resides in the DIN-PACS networks in the database archive systems and includes (a) patient demographics; (b) patient images from x-ray, computed tomography (CT), magnetic resonance imaging (MRI), and ultrasound (US); and (c) prior patient images and related patient history.
- Meta-Manager information to be protected consists of several data objects. This information is distributed to the Meta-Manager nodes and includes (a) radiologist schedules; (b) modality worklists; (c) routed case information; (d) DIN-PACS and CHCS messages, and Meta-Manager administrative and security information; and (e) patient case information.
- Access control and communications security is required in the VRE to control who uses the VRE and Meta-Manager facilities and to secure the messages between VRE components

The VRE provides teleradiology services to address the issues of cost, improved service quality, and medical access in the US Army (Fig 1). It is designed to provide store and forward, case review, and remote consultation and diagnosis capabilities. The VRE is a wide area network (WAN) that interconnects major US Army Medical Centers (AMCs), Army Community Hospitals (ACHs), and MTFs located in the GPRMC (Fig 2). Each MTF has a local DIN-PACS network designed for the effective acquisition, transmission, display, and management of diagnostic imaging studies. Within each facility, the DIN-PACS system is intended to eliminate the necessity of creating film and to allow access to images by multiple users simultaneously. Between facilities, the Meta-Manager system is designed to create opportunities to dynamically shift workload at any time and to any location based on a number of parameters (ie, availability of clinical expertise, case urgency, preferred radiologist, etc). The VRE enables improved radiology services to facilities with limited resources. It also grants access to specialists and particular expertise to all patients, regardless of physical location. The VRE effectively enables the US Army to make the most efficient use of their radiology resources and to give the best possible care to their patients. It also provides a means of connecting legacy databases for application of management tools.

OPERATING ENVIRONMENT

The VRE system consists of local DIN-PACS networks connected by a WAN, such as the T1 MedNet or continental United States (CONUS)-based asynchronous transfer mode (ATM) network. Figure 2 shows the initial testbed network for the VRE system. The VRE Meta-Manager manages the flow of cases and communication between DIN-PACS sites and other legacy PACS sites. A generalized high-level picture of three DIN-PACS networks connected via a private US Army Intranet is shown in Fig 1. The Meta-Manager follows a hierarchical architecture and is made up of client Meta-Managers (CMMs), regional Meta-Managers (RMMs), and a Master Meta-Manager (MMM). CMMs reside at each DIN-PACS site. RMMs control CMMs within the same region. The MMM has control between regions.

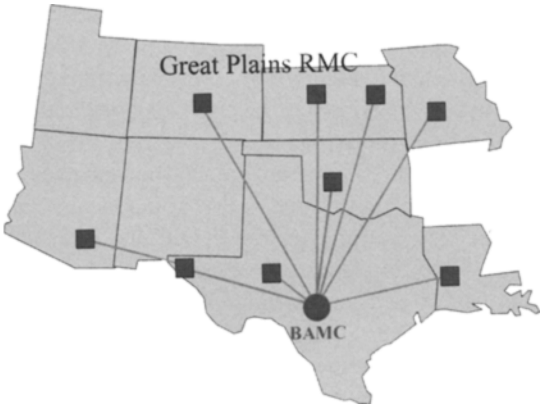

Fig 2. The VRE testbed in the GPRMC.

VRE SYSTEM ARCHITECTURE

The VRE system architecture consists of three major components: DIN-PACS networks at each MTF site where patient cases are originally acquired and stored; a private Army Intranet that is the communications network that connects the

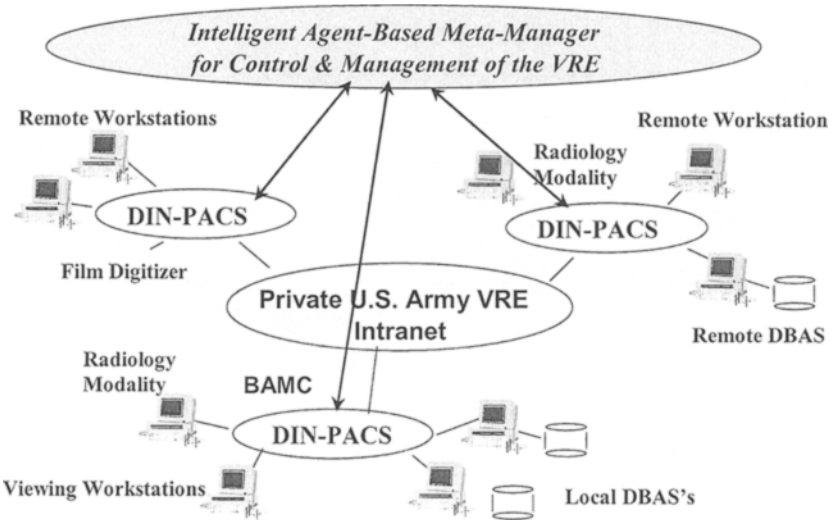

Fig 1. Overall VRE and Meta-Manager Systems.

VRE's MTF sites and is used to transport the patient cases between MTFs; and the Meta-Manager intelligent system that determines the DIN-PACS networks to be used to route patient cases for diagnosis.

In the VRE, the information to be protected is embedded in these three major components. The patient information consists of DICOM-formatted fields, such as patient demographics; patient images from x-ray, computed tomography (CT), magnetic resonance imaging (MRI), and ultrasound (US); and prior patient images and related patient history. The Meta-Manager information to be protected consists of several data structures, such as radiologist schedules; modality worklists; routed case information; DIN-PACS and CHCS messages; Meta-Manager administrative information; and patient case information.

DIN-PACS ARCHITECTURE

Each DIN-PACS is designed to be a standards-based system using proven commercial-off-the-shelf (COTS) subsystems such as DICOM, CHCS, Transmission Control Protocol/Internet Protocol (TCP/IP), Ethernet, ATM, IBM Unix, and Windows NT workstations. The DIN-PACS architecture is shown in Fig 3. It is composed of six major components: quality-control workstations, an archive, diagnostic/reviewing workstations, a high-speed local network, a teleradiology spoke, and a radiology information system (RIS)/workflow management server. These components communicate through DICOM, a standard used in the medical imaging community.

META-MANAGER ARCHITECTURE

The Meta-Manager follows a simple hierarchical structure (Fig 4). Client Meta-Managers reside at each DIN-PACS site. The sites are grouped into regions and the regions are managed by RMMs. A MMM controls interaction between regions. Within the GPRMC, the Meta-Manager architecture consists of one RMM and 10 CMMs. When the VRE is expanded to include more than one region, GPRMC's RMM will be connected to other RMMs via a MMM. Each Meta-Manager is placed on an NT workstation that is connected to an outside network for communication between Meta-Managers. The NT workstations are also connected to the local DIN-PACS networks via Ethernet.

VRE SECURITY POLICY

The VRE Security Policy was developed to cover the major VRE components: Meta-Manager, the VRE communications network, and the DIN-PACS networks. The VRE Security Policy consists of several related policy statements that address security features in each VRE component. This section summarizes a few policy statements. The VRE will provide protective measures, to include discretionary access control (DAC), identification and authentication (I&amp;A), audit, resource allocation, object reuse, communications security (COMSEC), and system and data integrity mechanisms. Physical and procedural security mechanisms will be employed wherever necessary to comply with GPRMC, DA, and DoD regulations.

These policies were formulated to comply with legal, regulatory, and operational information pro-

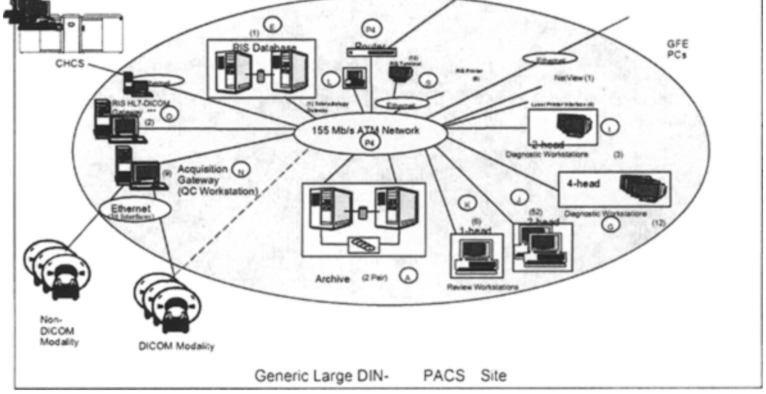

Fig 3. DIN-PACS architecture.

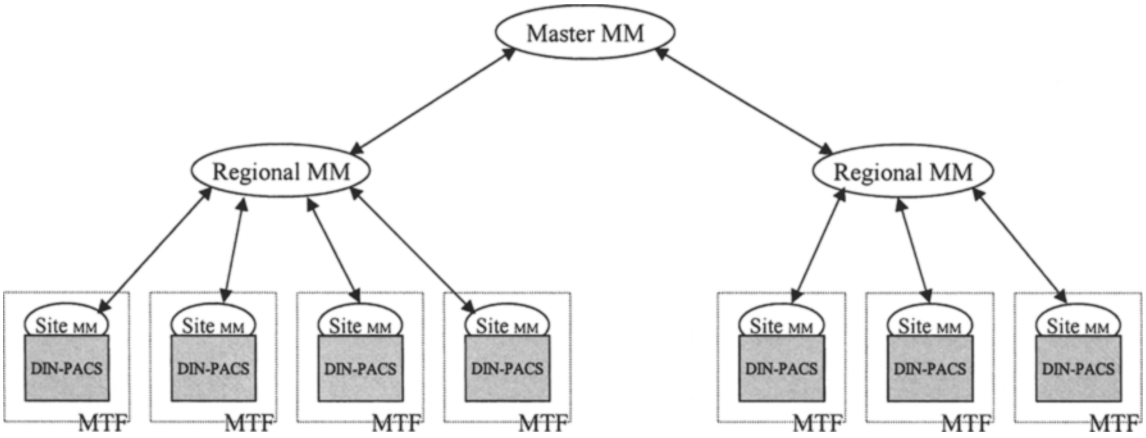

Fig 4. The 3 levels of the Meta-Manager hierarchy.

tection imperatives while providing continued availability of VRE system services to authorized users.

CONFIDENTIALITY

The following policy statements provide for the control of information access so that only authorized persons or mechanisms may view or modify the data.

Policy Statement No. 1

The VRE configuration shall implement all Controlled Access Protection requirements, Class C2, per TCSEC and AR 380-19. This means VRE security policy shall require implementation of DAC and object reuse mechanisms. Mechanisms to provide for accountability shall include identification, authentication, and an audit trail capability. The system architecture design will ensure the implementation of resource isolation to protect resources that are subject to audit and access control requirements. In addition, the development/ installation acceptance team will complete security testing to ensure that security mechanisms work.

Policy Statement No. 2

The local commander or his authorized designated representative shall ensure the protection of VRE information in accordance with (IAW) the Privacy Act of 1974.

Policy Statement No. 3

VRE information containing patient identifiable data must be encrypted for transmission between sites.

Policy Statement No. 4

A Systems Interface Agreement (SIA) will document any external connections to the VRE system.

Policy Statement No. 5

The local commander or his designated representative will train and monitor VRE users in their security responsibilities in relation to the VRE system and the protection of the sensitive information.

Policy Statement No. 6

The local commander or his designated representatives will ensure that only authorized maintenance personnel perform maintenance on the VRE system. Individuals with the technical expertise to detect obvious unauthorized modifications must escort and observe all maintenance personnel during maintenance operations.

Policy Statement No. 7

The VRE system administrator (SA) will ensure that VRE data output is marked with the appropriate sensitivity level (eg, For Official Use Only [FOUO]). VRE data output includes data that are viewable on a monitor. A system warning regarding the proper handling of sensitive information at log-in time is sufficient to meet this requirement for monitor output. This applies only if the reports are not already annotated by the system. A cover sheet marked with the appropriate sensitivity level should be printed as the first sheet of each print job. Individual sheets should also be marked in a manner that will not interfere with the readability of the printed information.

Policy Statement No. 8

Information Systems Security Officers (ISSOs) shall promulgate proper procedures for authentication data (eg, passwords) management, generation, composition, periodic change, and compromise. The procedures shall be in proper accordance with applicable DA and DoD regulations.

Policy Statement No. 9

The VRE program developer shall implement appropriate account lockout procedures and warning banner to deter unauthorized access attempts. The VRE Administrator is responsible for ensuring that these mechanisms are properly implemented throughout the system.

INTEGRITY

The following policy statements provide protection against modification or corruption of information, either maliciously or accidentally.

Policy Statement No. 10

The VRE architecture will maintain a domain for its own execution that protects it from external tampering or interference.

Policy Statement No. 11

The ISSO shall implement measures to protect the integrity of trusted hardware, firmware, and software. This will include either automated function to allow for periodic validation of the hardware, firmware, and software elements of the computing base, or written directions on how to accomplish this validation.

Policy Statement No. 12

The VRE SAs shall control the hardware, software, and documentation configuration such that only authorized changes are allowed.

Policy Statement No. 13

Only personnel who have the proper clearance, authorization, and need-to-know (need-to-access) for the data being modified or deleted will be allowed to change data within the VRE.

Policy Statement No. 14

The VRE shall provide protection against modification of data during transmission.

Policy Statement No. 15

The VRE shall detect unauthorized attempts to modify data. Procedures for investigating unauthorized access attempts shall be documented.

Policy Statement No. 16

The VRE system will be protected from modification and/or destruction from viruses, Trojan horses, worms, etc.

Policy Statement No. 17

The VRE system will include the capability to audit all security-relevant events. The system documentation will include a comprehensive audit strategy that includes which activities to continuously/periodically monitor, or only audit upon suspicion of unauthorized activity.

Policy Statement No. 18

Audit data will be protected from modification and unauthorized access.

Policy Statement No. 19

The VRE will retain the audit data for at least 180 days.

Policy Statement No. 20

The audit information will be reviewed at least once a week.

AVAILABILITY

The following policy statement provides for the availability and timeliness of VRE data. Availability is the ability of the system to keep working efficiently and to keep information accessible. For this security policy, availability also addresses denial of service: an action or series of actions that prevents the system or any of its resources from functioning efficiently and reliably.

Policy Statement No. 21

The VRE will implement appropriate measures to ensure system resources are available when needed. These measures will include backup/recovery features, diagnostic features, contingency planning and measures, and access controls.

VRE USER POLICY

All VRE users will follow the following policies relating to VRE security.

(a) The ISSO, Director of Information Management (DOIM), and SA for the MTF site will act in their respective roles for the VRE system at that site as well.

(b) Each individual user of the VRE system will be assigned his/her own user identification and password for the system.

(c) When users leave their workstations or personal computers, they will log-off or lock the keyboard and screen until they return to the workstation and reauthentication is performed.

(d) Workstations and personal computers will include a local "idle lockout/screen saver" feature that automatically locks the screen and keyboard after a specified period of no activity, requiring reauthentication before unlocking the system (eg, a password-protected screen saver).

(e) When computer viruses are detected, they will be immediately reported to the site ISSO and DOIM.

(f) VRE sites are assumed to have an individual or group of individuals in charge of network maintenance. This individual or group will be referred to as the Network team. When any VRE user receives an announcement about viruses from any source other than the Network team, he or she will forward the warning to the Network team only for verification and notification.

(g) An end-of-day security check will be performed each day. The site ISSO will determine the responsibilities of the end-of-day security checker and will post them in a highly visible place with an end-of-day security checker roster.

(h) VRE hardware will be kept in a confined area. An area is considered to be confined if it is not readily accessible to individuals without the authorization to use it.

(i) A security incident is any security policy violation. Security incidents will be handled with a "protect and proceed" policy. If a security incident is detected, measure taken to protect the system's resources will take precedence over those taken to identify the policy violator.

(j) Should a security incident result in identification of a system's vulnerability, the VRE Administrator must be notified. The notification should include any implemented or recommended solutions to the vulnerability.

USE OF THE CORBA SECURITY SERVICE

The VRE Security Policy is the first attempt to define the security infrastructure for the VRE Project. In this section, we describe how the CORBA Security Service is to be used to implement the policy. First, a security process model will be prepared which will as realistically as possible describe security administration of the VRE Meta-Manager prototype. This process model will use unified modeling language (UML) syntax to describe the process architecture. Second, a multiple Internet protocol (IP) domain-capable version of one or more of the present VRE prototypes will be tested and fielded. This version will then be modified with a CORBA security system to create a Multiple Domain Security Platform for CORBA–based Applications, or MDSCAP. The MDSCAP security model will be based on that presented for the SCAP in the Meta-Manager Design Specification. This will allow a commercial security product to be further evaluated as it applies to the VRE Meta-Manager system. This will determine how well a security process model that meets the requirements in the VRE Security Policy and the Meta-Manager Design Specification may be implemented using the commercial product and how well the commercial security software will work in a VRE Meta-Manager prototype system.

The VRE project's security policy and requirements are summarized and possible applications of the CORBA Security Service to the VRE project are discussed. In this task, we will determine which service can enhance the C2-level security requirements in the VRE system. Because the CORBA Security Service provides a flexible security framework, most of the VRE project's security requirements can be met within the context of CORBA. We start with a baseline security architecture defined by the SCAP, which was proposed to support CORBA Security in distributed and standalone CORBA-compliant systems. Four functional blocks provide security services: the Authentication Block, the Security Association Block, the Access Control Block, and the Security Information Management Block. In addition to a client machine and a server machine, the platform requires a domain security server to support necessary third-party functions such as authentication, cryptographic, and security administration services. Figure 5 shows the interaction of the main security components in the SCAP.

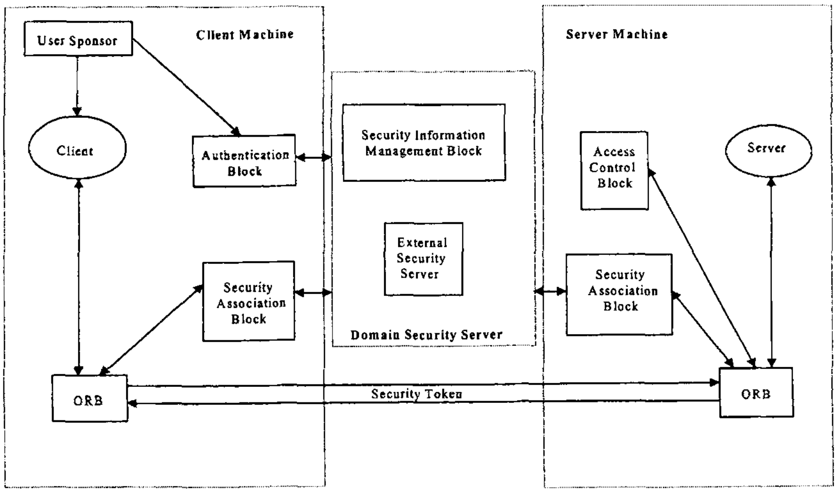

Fig 5. The Security Platform for CORBA-based applications (SCAP).

IDENTIFICATION AND AUTHENTICATION

The VRE Project requires its users to be authenticated to the system and its objects to be authenticated to each other (peer entity authentication). As shown in Fig 6, CORBA authentication is done using UserIDs and passwords through a UserSponsor object. The Principal Authenticator generates all UserID/Password information. Each UserID/Password pair will be validated and matched with a particular set of user privileges (based on the principal's role). As required by DII-COE standards, CORBA also has the ability to use X.509 version 3 certificates (supported by Java over CORBA [COE97]). CORBA security provides peer entity authentication using its security association services. The services are accessed when making a secure object invocation. Security associations are created using key distribution and certification authorities for public keys. They provide both unilateral and mutual authentication. By using the principal authentication services and security associations offered by CORBA, the identification and authentication requirements of the VRE Project can be met.

ACCESS CONTROL

Access control is required in the VRE to limit the access to system resources of DIN-PACS, the Meta-Manager, and the associated knowledge bases. In the CORBA Security Service, access to system objects is based upon a principal's rights or privileges (discretionary control). The privileges given to a principal may be assigned based upon the "groups" that an individual belongs to. The CORBA Security Service keeps access control lists in order to allow privileges based upon groups. These privileges are defined in the Credentials object. Because the Credentials object is created upon authentication of the user, any principal with Credentials can be considered authenticated. Access

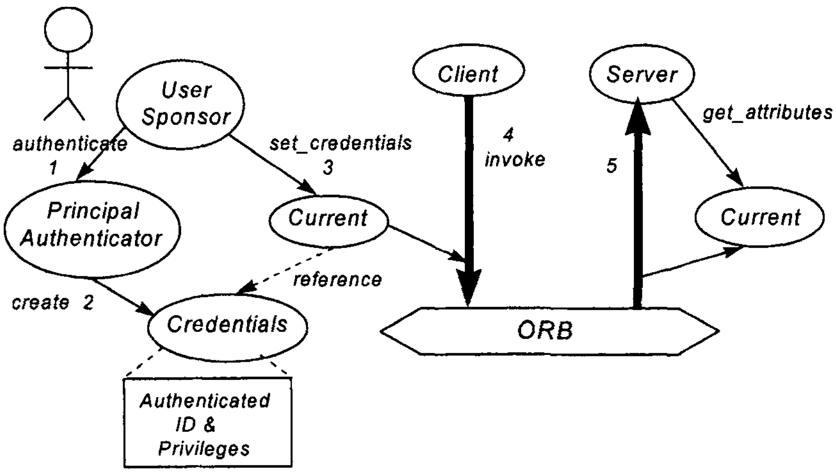

Fig 6. Identification and authentication using CORBA.

decisions can be made at both the client and server side. All access decision functions should deny any rights that are not specifically given by the principal's privileges. The object invocation access policy should allow only authorized personnel to access teleradiology data. This will be enforced by the client-side object invocation access decision based on the principal's Credentials object. The ability to change DIN-PACS or Meta-Manager data should be controlled by the target application access decision. The application access decision can control access to particular methods or particular data types. When needed, the simple delegation method should be used to delegate authority to intermediate objects in an object chain (in order to base invocation on the principal's privileges). Because object invocation in a secure ORB is based on a defined set of privileges, access control can be managed to a fine level of granularity. The access control requirements of the VRE can be satisfied by the CORBA Security Service.

COMMUNICATIONS SECURITY

The VRE requires data integrity and confidentiality services in communications messages over the virtual private network. CORBA provides these services through encryption and cryptographic checksums. According to the DII-COE standard, the VRE must provide each user with a private key. CORBA can support a Kerberos public/private key mechanism to meet this requirement. Communications security can also be provided through security association services. CORBA security is security technology independent so that it can support numerous encryption algorithms for data confidentiality. It also supports hashing functions to insure data integrity. In general, CORBA provides communications security by supporting the services offered by established mechanisms. Using these mechanisms, we will provide for the confidentiality and integrity requirements for messages and communications between the VRE nodes.

POSITIVE BINDING OF PATIENT INFORMATION

The positive binding of patient information is a very important VRE security requirement. It is provided through a digital signature or cryptographic process. As with communications security, the CORBA Security Service can provide these types of mechanisms for positive binding of patient information. Patient information should be kept within the same security technology domain. A unique digital signature can be assigned to each patient's information. The signature will be used to bind the data together. The CORBA Security Service can also support standard electronic signature mechanisms.

SYSTEM AVAILABILITY

The protection of system availability is also a VRE requirement. CORBA cannot directly provide services for this protection. The best way to guard system availability is to design the network to be as fault-tolerant as possible. CORBA can contribute to the ability to react to a system availability problem. The DII-COE standard requires system administrators to be notified when a system service has failed. We will use the features of the VisiBroker's Smart Agent, or OSAGENT, to implement fail-safe operation of the VRE nodes and workstations. The OSAGENT works between client and workstation to detect and alert personnel when an object implementation or client has gone down. This feature circumvents the requirement to monitor the status of the VRE's communications network to determine when a link or node has gone down. In addition, the VisiBroker's Object Activation Daemon (OAD) may be used to determine the policy for how failed or new nodes are restarted and introduced into the VRE system, respectively. The OAD enables us to define an object activation policy for each Meta-Manager node so that when the object implementation is not running or has failed it can be reactivated according to this policy.

FIREWALLS IN THE VRE

The DIN-PACS networks in the VRE will be protected in the future by firewalls at the hospital entrance of the VRE communications network. In this project, we will determine the features of CORBA that need to be implemented to interact with the firewall. The CORBA/Firewall Security Specification defines a manner in which clients can have better accessibility to CORBA application servers behind a firewall. The goal is for client-firewall-server communication to be more easily enabled and controlled in a more comprehensive set of circumstances. There are three main aspects considered in the specification: changes in the format of Interoperable Object References (IORs) to include firewall addressing information, support for Internet Interoperability Protocol (IIOP) over Secure Socket Layer (SSL), and support for callbacks between servers and clients.

IORs are object profiles that describe how to contact the same object using a particular ORB's mechanism. Essentially, IORs support CORBA's ability to allow clients to invoke methods without knowing the location of the server. Whenever an object reference is passed across ORBs, an IOR for that object must be created. The IOR maintains a collection of tagged profiles that provide self-describing data identifying the object reference's ORB domain and the protocols that it supports. It contains information about the target address of an object, such as the host address and port. In order to support firewall traversal while accessing an object, a tagged component including firewall information has been proposed. The tagged component includes the sequence of firewalls that protect the target object and the firewall types. Thus, the IOR contains information for the ORB that will allow the correct host/port combination to be used to traverse the firewall and access the correct server using IIOP.

The second issue addressed by the CORBA/Firewall Security Specification is IIOP/SSL. SSL is a security mechanism that was designed to provide reliable end-to-end communications security over TCP. It can provide data encryption, server authentication, message integrity, and client authentication. Because its use is so widespread, SSL is a strong candidate for the support of secure method invocations in CORBA. Thus, the ability for firewalls to support IIOP/SSL communications is in direct alignment with the ability to support secure method invocations. The methods in which IIOP and IIOP/SSL are handled by a firewall are necessarily different. Because IIOP/SSL communications will be encrypted, the firewall will not be able to conduct content checks to ensure communication legitimacy. However, because SSL provides its own authentication between the client and server, this is not seen to be a problem. The proposed mechanism for IIOP/SSL communication is a General Inter-ORB Protocol (GIOP) Proxy. GIOP is a set of message formats and data representation for ORB to ORB communications. IIOP is essentially GIOP designed to run over TCP/IP. A GIOP Proxy can be used to create a pass-through connection based on an access control negotiation at connection setup. A pass-through connection does not require the Proxy to check the connection content, only whether or not the connection is allowed. The final issue addressed by the CORBA/Firewall Specification is the ability to support callbacks. Callbacks are used when it is desirable for an application server to contact a client to facilitate asynchronous information flow. The problem that arises in this case is when a firewall protecting the client object allows outbound connections, but does not allow inbound connections. Thus, the callback connection request from the server to the client will be blocked by the firewall. To address this issue, bidirectional GIOP or bidirectional IIOP has been suggested. Using bidirectional communication, the server object can reuse the client's connection to send request messages.

The CORBA/Firewall Specification focuses on interoperability and on leaving room for proprietary development. Much greater flexibility is granted when dealing with a solution to a specific implementation such as the VRE. The CORBA/firewall design outlined in this section combines features from VisiBroker's Gatekeeper and from two distributed security frameworks. The design has been developed so that its implementation can support the CORBA Security Service as a whole.

We have elected to use the VisiBroker ORB and

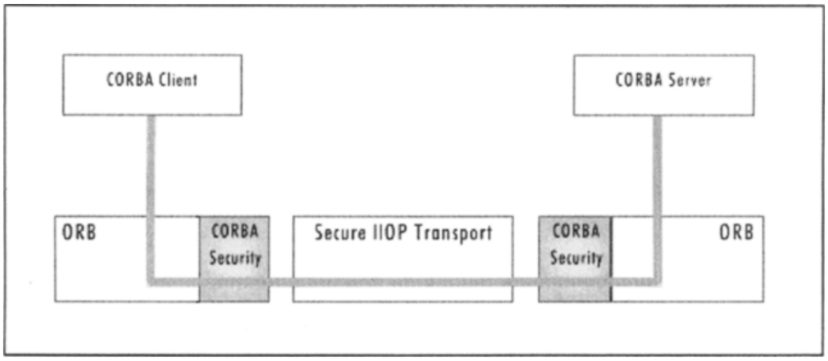

Fig 7. Overall secure object processing in CORBA.

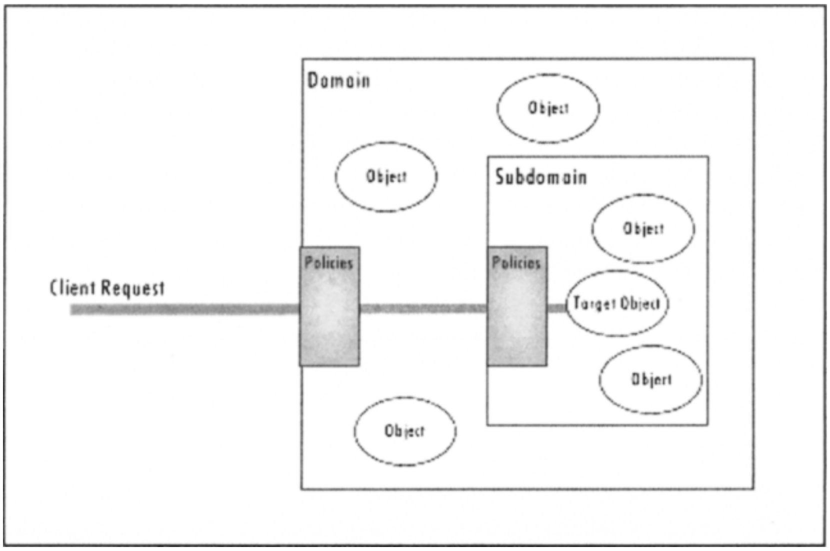

Fig 8. Gradient domain policy of the VRE.

will buy the VisiBroker Gatekeeper as a part of their ORB package. The Gatekeeper allows CORBA communication with objects behind a firewall. The Gatekeeper sits on a server outside of the firewall and acts as an IIOP proxy. It wraps IIOP messages in HTTP packets, creating an "HTTP tunnel." The firewall can be configured to pass HTTP packets from the Gatekeeper, thus, allowing IIOP communication over the firewall. The Gatekeeper can be implemented in several different firewall architectures. The Gatekeeper may be implemented as a proxy server behind a packet filter. This implementation is of particular interest because it is one of the motivators behind the CORBA/Firewall design for the VRE. The Gatekeeper can also be run on a bastion host directly behind a packet filtering firewall. When starting the Gatekeeper, it is important to specify an IP address, an exterior port, an interior port, a callback port, and a forward port. The exterior and interior ports are used to accept connections from the client and server respectively. A callback port is used to support invocation of

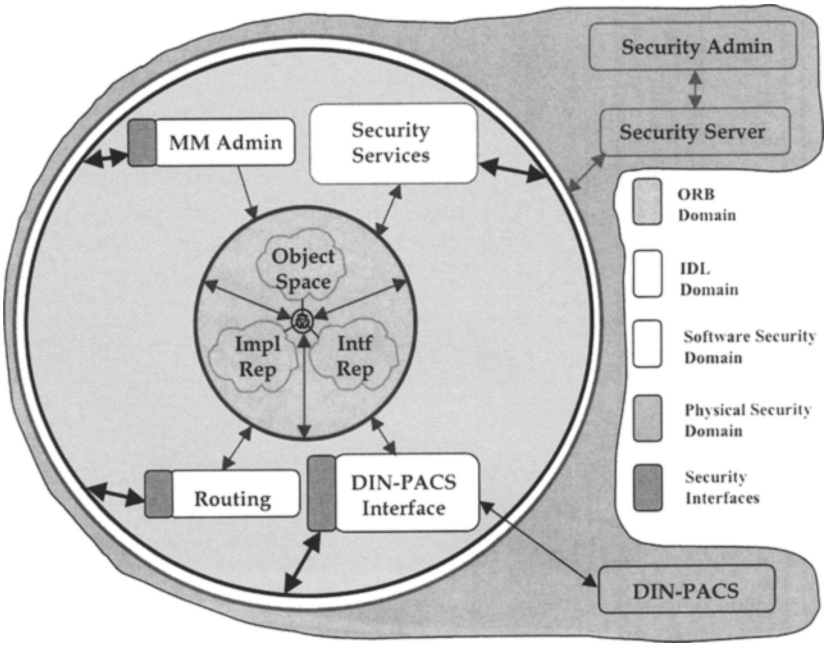

Fig 9. Overall design for the VRE Security architecture.

callback objects. Several forward ports may be specified. They are used by the Gatekeeper to forward calls from a web-based application or Java applet to server objects. In the packet filter architecture, the firewall can filter IP packets to the Gatekeeper for calls on the exterior port. The default for the exterior port for the VisiBroker Gatekeeper is 15000. Assuming a well-known IIOP port, all traffic coming in on that port can be directed to the Gatekeeper's exterior port to be handled by the IIOP proxy. In the case where the firewall cannot handle IIOP traffic, HTTP tunneling will have to be used.

GRADIENT SECURITY SERVICES SOFTWARE

The VRE Project evaluated several CORBA Security Service software systems and selected the Gradient, Inc (Cambridge, MA) product. NetCrusader/CORBA supports the Level 1 and Level 2 security functionality described in the Object Management Group's CORBA Security Service (Version 1.5) specification. This allows clients to invoke target objects over a Secure Inter-ORB Protocol (SECIOP) link, and servers to perform access control and auditing when a client invokes a target object. NetCrusader/CORBA runtime components integrate into the client and server ORBs to establish security contexts, manage the state of those contexts, and provide the required security by reading policies and communicating with the security server. NetCrusader/CORBA uses an underlying Kerberos framework for confidentiality and the generation of credentials for authentication and authorization. Figure 7 illustrates how requests by an application client for objects on an application server are handled securely over the network. A security policy domain is a group of application objects to which you apply common security policies. Creating domains is the principal method you use to structure and administer your CORBA security environment. Domains simplify administration by allowing you to apply access control, authentication, delegation, and auditing policies to groups of objects at once. Application objects are added to domains on the application side using command line options. All objects created by this server will be members of a given domain and subject to the security policies you apply to that domain. NetCrusader/CORBA supports hierarchical domains as described in the CORBA Security specification. Hierarchical structuring of domains allows security policies to be implemented globally by nesting subdomains within domains, as shown in Fig 8. Subdomains inherit the parent domain's security policies, but a subdomain's policies can differ from and override the parent domain's policies. The VRE security architecture will use the multiple domain system.

SUMMARY

This report gives an overall description of the VRE security policy and the CORBA security services that are used to implement it. Figure 9 shows the overall approach that we use to develop the CORBA security architecture for the VRE Project and components. The material is too vast to present in detail and only a summary description is given here. For more details, readers should refer to the reference material for the VRE Project.