Security Model for Picture Archiving and Communication Systems

Douglas B. Harding Jr, Robert J. Gac Jr, Chester T. Reynolds III, John Romlein, and Anna K. Chacko

The modern information revolution has facilitated a metamorphosis of health care delivery wrought with the challenges of securing patient sensitive data. To accommodate this reality, Congress passed the Health Insurance Portability and Accountability Act (HIPAA). While final guidance has not fully been resolved at this time, it is up to the health care community to develop and implement comprehensive security strategies founded on procedural, hardware and software solutions in preparation for future controls. The Virtual Radiology Environment (VRE) Project, a landmark US Army picture archiving and communications system (PACS) implemented across 10 geographically dispersed medical facilities, has addressed that challenge by planning for the secure transmission of medical images and reports over their local (LAN) and wide area network (WAN) infrastructure. Their model, which is transferable to general PACS implementations, encompasses a strategy of application risk and dataflow identification, data auditing, security policy definition, and procedural controls. When combined with hardware and software solutions that are both non-performance limiting and scalable, the comprehensive approach will not only sufficiently address the current security requirements, but also accommodate the natural evolution of the enterprise security model.

Copyright © 2000 by W.B. Saunders Company

NEW TECHNOLOGICAL ADVANCES in the storage, transfer, and retrieval of data have created both the dream of unparalleled opportunities to share data almost instantly and the nightmare of unauthorized and unplanned leakage of private information. To take advantage of the former and avoid the latter requires a careful and systematic approach to security concerns in both the initial stages of system installation and life-cycle management of operations. This security model is a multi-tiered approach with public key infrastructure (PKI) as the foundation. Internal threats or

vulnerabilities to physical assaults must be addressed by other means. For instance, basic personnel and procedural security policies must be crafted, implemented, and enforced to demonstrate an organization's commitment to prevent breaches of security.

BACKGROUND

In 1996, Congress recognized security concerns by enacting the Personal Privacy Act (PPA) and the Health Insurance Portability and Accountability Act (HIPAA). These acts were designed to hold medical institutions to a high level of accountability for safeguarding patient information. The US Army is implementing a picture archiving and communications system (PACS) as part of its Virtual Radiology Environment (VRE) Project at 10 medical facilities in the Great Plains Regional Medical Command (GPRMC). To stay compliant with new legislation, the VRE Project could be required to secure and track patient records that need to be stored, as well as transported across the VRE domain. These records would include imaging studies, study reports, and associated metadata.

INITIAL SECURITY STEPS

Two security measures form the foundation in creating a sustainable risk-controlled environment capable of maintaining accountability and audit control: (1) Isolation of data storage through hardware-based "firewall" protection, with passwords using modern encryption safeguards, is mandatory. (2) As a baseline, an organization must be able to control all web, E-mail, file transfer protocol (FTP), and Telnet access. Additional security measures need to be implemented to ensure a complete security model.

A "firewall" is the first step in protecting a system. By establishing a single controllable interface between the facility and the outside world, one can provide a foundation for securing wide area network (WAN) traffic (Fig 1).

Complex alphanumeric passwords, which use a minimum of eight characters, including at least one capital letter and a number, and are changed every 45 to 60 days, are a minimal way to secure¹ local area network (LAN) traffic. For auditing clinical

From InformaTech, Inc, Frederick, MD; and United States Army Medical Research and Materiel Command, Ft Detrick MD.

Address reprint requests to Douglas B. Harding Jr, Network Engineer, InformaTech-Telemedicine Services, 5300 Westview Dr, Suite 408, Frederick, MD 21703; E-mail: Douglas.Harding@iti-tmed.com.

Copyright © 2000 by W.B. Saunders Company
0897-1889/00/1302-1051\$10.00/0
doi:10.1053/jdim.2000.6882

Fig 1. PACS enterprise security model.

information, every user must have a unique user-ID and password. Almost every operating system has the ability to track its users and to limit them to specified resources by way of user profiles. When there are many disparate systems or different kinds of operating systems in the same facility, a central lightweight directory application protocol (LDAP) can be used to store (for each user) permission certificates that determine which areas may be accessed.

Limiting incoming and outgoing transactions is important to maintain security, but can create serious impediments to conducting business in a timely manner. Virtual private networks (VPN) are a tool for controlling communications external to a LAN. However, these links, which can be established and broken on demand, should incorporate the use of sophisticated encryption packages² (Fig 1).

SECURITY POLICY CONSIDERATIONS

The goals of the VRE Project are to dynamically distribute images and patient information within an individual hospital and regionally linked facilities; to enhance productivity, training, workflow, timeliness, and military readiness; and ultimately to improve patient care. By linking individual systems together, it becomes clear that secure WAN connectivity must be included in the architecture, not only for site-to-site communications, but also for remote maintenance activities by vendors.

SUMMARY

The VRE Project faces several challenges that must be met to retain the certification for the military, as well as the more stringent requirements of HIPAA and the PPA of 1996.³ Fundamental but not necessarily simple steps are to (1) identify the areas of information that need to be protected; (2) decide what data needs to be tracked; (3) define how information must flow in order to perform its function; (4) develop policies that will be consistent within the new security umbrella; (5) create procedural controls that will avoid omissions or inconsistencies; and (6) create appropriate personnel policies restricting access and use of private information. Completing these steps will allow the VRE Project a security posture that will enable productive workflow while protecting the project from harmful and costly security attacks and leaks.

REFERENCES

1. The NSA Rainbow Series Orange Book. URL: <http://www.fas.org/irp/nsa/rainbow/tg006.htm>
2. The NSA Rainbow Series. URL: <http://www.fas.org/irp/nsa/rainbow.htm>
3. Saul J: HIPAA Security and Electronic Signature Provisions—Executive Summary. Communications Technology Consulting and Jerboa, Inc, 1999. URL: <http://www.Jerboa.com/hipaa>
4. Epstein MA, Pasioka MS, Lord PM, et al: Security for digital information age of medicine: Issues, applications, and implementation. J Digi Imaging 11:33-43, 1998