PCASSO: A Model for Safe Use of the Internet in Healthcare

by Dixie B. Baker, PhD

Can the Internet support a system that gives both providers and patients safe access to clinical data? That's the goal of the PCASSO project. Here's how this real-life trial of an Internet patient information system works.

In recent years, the rapid development of Internet technology has spurred a new trend in healthcare-empowered consumers and networked care providers. The public has embraced personal computers and connectivity, and this same networking and information technology is making its way into physicians' offices and other healthcare organizations. The exploding popularity of the World Wide Web and e-commerce push healthcare providers to pay serious attention to this electronic phenomenon for providing quality healthcare at a reasonable cost.

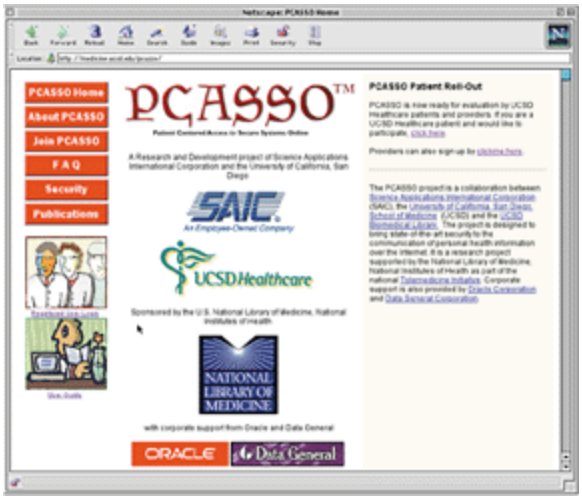
At the same time, the industry recognizes the need to balance potential benefits against risks to personal privacy, data corruption, and service interruption. Concern over these risks prompted Congress to include a security standard and privacy provisions among the mandates prescribed by the Health Insurance Portability and Accountability Act (HIPAA).

The problem facing healthcare today is capitalizing on Internet and Web technologies to improve quality, lower costs, enable telemedicine, and provide consumer health services while protecting confidential information, patient privacy, and human safety. This article describes one attempt to address these issues through a real-life trial of an Internet patient information system.

To test technical and organizational approaches to safeguarding personally identifiable electronic health data accessed over the Internet, the National Library of Medicine (NLM) awarded Science Applications International Corporation (SAIC) and its partner, the University of California, San Diego (UCSD), a research and development contract under its health applications for the national information infrastructure (NII) initiative. The resulting project is described in this article.

E-commerce Limitations

The Internet was designed by the scientific and academic communities to allow efficient and open information sharing among "trusted" entities. Little thought was given to protecting sensitive information. Its designers could not have foreseen that the Internet would expand to virtually connect all of the world's public and private networks.



Vulnerabilities in applications available over the Internet further complicate matters. The most common application is the Web, which is now a driving force in information technology development. But the simple, free-floating Web has serious drawbacks when applied to distributed, enterprise computing for healthcare.

Internet security technologies tackle some of these weak points. The secure sockets layer (SSL) protocol and the Internet Protocol Security (IPSec) standard, for example, address end-point authentication and confidentiality of Internet protocol datagrams or "packets." But these technologies don't address user authentication or end-point vulnerabilities.

Many healthcare organizations look to electronic commerce (e-commerce) solutions to provide security solutions that will allow them to securely use the Internet and the Web. SSL, the protocol used most extensively, is designed to authenticate end points (client authentication is optional) and encrypt the connection. But SSL does not address end-point protection; once a message arrives at the server, it is decrypted and exposed to potential hackers. The Secure Electronic Transaction (SET) protocol, designed to protect credit card information, similarly does not address the protection of end-point environments.

Healthcare is very different from e-commerce in several ways. Most importantly, a loss is irrecoverable. The disclosure of one's genetic footprint or mental health record can change an individual's life forever, potentially affecting employment, financial status, and ability to get a job. Healthcare also involves multiple levels of sensitivity, some of which require special protection by law.

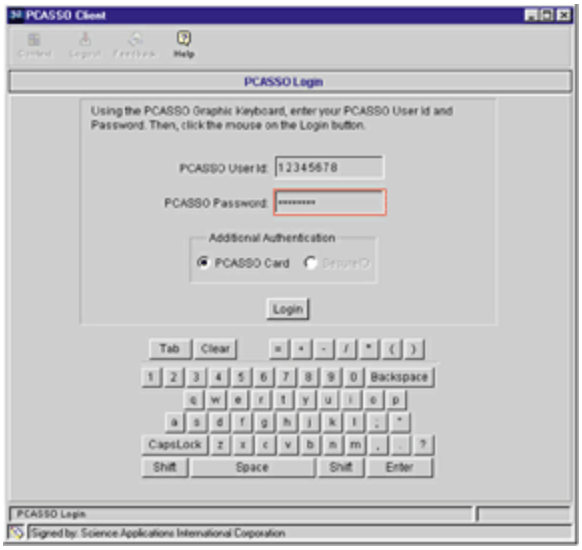
The PCASSO Project

SAIC and UCSD conceived an experiment called Patient Centered Access to Secure Systems Online (PCASSO). The purpose of the experiment was to determine whether state-of-the-art security technology and assurance methods that, at the time, had not been applied in healthcare, would enable consumers and their providers to access highly sensitive patient information on the Internet safely and effectively. The two entities worked together to research, develop, deploy, and evaluate PCASSO. The project began in October 1996 and continued through September 1999 and was funded by the National Library of Medicine at the National Institutes of Health.

Investigators wanted to test these hypotheses:

- The Internet can support an information access and distribution model that gives healthcare providers and patients secure, selective access to person-specific clinical data
- The PCASSO model is a safe and effective way to communicate clinical information as part of the healthcare a geographically dispersed organization delivers
- Medical librarians' knowledge and skills can help the Internet-empowered lay public find an unprecedented amount of health-related information, including that in their own medical records

PCASSO was publicly funded, and any solutions it produced needed to be applicable and adaptable to a broad range of organizations and computing environments beyond UCSD.



Because PCASSO users would include providers and patients, the system needed to be acceptable to—and usable and safe for—both groups. The design had to strike a balance between safety and usability. A highly secure system that no one used was out of the question.

Finally, users should not need to buy any special equipment, although it clearly would have been easier to achieve PCASSO's objectives if users had been required to purchase hardware encryption devices or diskless network computers.

PCASSO is an important innovation because it gives consumers easier access to, and more control over, their own medical information, assures that only specifically authorized individuals can access health records, and provides end-to-end accountability as required by the HIPAA security standard.

The model system has been running at UCSD since February 1999 and contains the complete records of more than 178,000 patients, with nearly 300 active users, including providers and patients. PCASSO allows users to search and view their electronic health records, including patient demographics, medications, lab tests, and transcription reports, through a familiar Web interface.

How It Works

At UCSD, PCASSO recognizes four user roles: primary care provider (PCP), secondary care provider (SCP), emergency care provider (ECP), and patient. Each role has a particular set of transaction capabilities. For example, one cannot assume the role of "PCP for all patients," but if authorized, one can assume the role of "PCP for Patient A." Multiple providers may have roles associated with one patient, but any single provider will have only one role associated with a given patient.

PCASSO controls access within sensitivity levels and categories. As configured for the UCSD trial, PCASSO recognizes five levels of information sensitivity:

- **low**—information that cannot be identified with a patient
- **standard**—information that can be identified with a patient
- **public**—deniable-information about conditions, such as HIV/AIDS, abortion, adoption, mental health, genetic, substance abuse, and sexually transmitted diseases, that by law requires special protection
- **guardian deniable**—information, such as that about teenage abortion, that can be denied to a guardian
- **patient deniable**—information that, if disclosed to the patient, might harm his or her well-being

The capabilities associated with each role are:

- a PCP can access all of a patient's information, upgrade or downgrade the sensitivity level of the patient's information, and give other providers a PCP or SCP role in dealings with that patient
- an SCP can access all information about a patient
- an ECP can assume the SCP role for a patient for 72 hours. All actions are audited, and role misuse can be detected
- patients can access all of their own information—except that which is patient-deniable-including the audit of accesses to it and a list of users who can access it

The role definitions and the rules associated with each role are specific to an organization. The definitions above reflect the UCSD configuration. However, PCASSO's design can accommodate many more roles and whatever security policy the organization wants to enforce.

New PCASSO account holders receive:

- a personal ID and password
- a read-only diskette with the person's private key and encrypted certificate and the PCASSO server's public key and certificate
- a laminated challenge-response card with a list of random numbers, each of which is used only once for logon
- the appropriate user guide
- a compact disc containing Netscape Communicator/ Navigator 4.0 to ensure that the browser supports signed Java applets

Typing in PCASSO's Web address and connecting with the server downloads a cryptographically signed Java applet (small application) that controls the client computer. On a graphical (on-screen) keyboard, the user enters an ID and password. PCASSO asks that the diskette be inserted, which establishes an encrypted link between the server and client computer. The server then "challenges" the user to enter a number as it appears on the laminated card.

The server presents a menu of possible "contexts:" provider, emergency, and patient, each of which is associated with a specific graphical user interface (GUI). Once a user selects a GUI, it must be associated with a particular user. If the user is a patient, this is done automatically. Otherwise, the user must enter the patient's name, a medical record number, or the first few letters of a surname in order to select a patient. The server lists the patients with whom the user has an established relationship, and one is chosen. Now the user has a defined role for viewing information.

Patients and providers have access to the same data as that stored in the UCSD clinical data repository; providers get to it internally through the UCSD clinical information system.

The user selects a labeled tab—such as demographics, visit, lab, radiology, cardiology, ops, or discharge—according to the kind of information she seeks. Through the GUI, the user can perform all actions she is authorized to perform in her current role. If a provider wants to change roles—say, from PCP for Patient A to SCP for Patient B—she can without logging off. Or if she wants to change GUI contexts—from PCP for Patient A to Patient, for example—again she can do so without logging off. The user logs off after completing her work.

Patients can see an audit trail showing who has looked at their medical records and who is allowed to do so. Whenever PCASSO detects a change in those records, it generates and e-mails a notification to the patient. The message doesn't explain the nature of the change, just that a change has occurred. Patients can select how frequently they want to be notified about changes.

Putting It Together: Design and Implementation

PCASSO's architecture includes an application server that provides a trusted domain to which UCSD's enterprise information systems pass data. These user data are sent to authenticated and authorized users via the Internet.

The firewall protecting other parts of the university's information system is behind PCASSO rather than in front of it, as is typical, because PCASSO, situated directly on the Internet, has its own built-in security safeguards. This architecture combines secure Web services, a trusted application server, and secure administration services to ensure that access to certain information is restricted to authorized individuals. The user connects to PCASSO by typing PCASSO'S universal resource locator, or URL. The Web server then sends back the Java applet, which from that point on communicates only with the trusted application server.

This server receives the user's requests, determines what data they can see and what actions they can perform and returns the results. Together, the components provide all of the major security services: authentication, access control, confidentiality, integrity, attribution, and availability.

Making Sure: Assurance Methods

Functionally, PCASSO uses the same security protections as many other Web-based health applications. The SSL protocol achieves client-server authentication and establishes a secure channel by combining a system-generated encryption key and a challenge-response token for user authentication. The application is contained within a Java applet that is downloaded from the server and runs on the client machine within a "sandbox" or safe area from which it can access only those system resources specifically made available to it. Like many other healthcare Web applications, PCASSO enforces a role-based access-control policy and audits user actions.

A primary difference between PCASSO and most other secured healthcare applications is label-based access control, which strongly isolates each hierarchical level of trust (low, standard, public-deniable, guardian-deniable, and patient-deniable). In addition, the label-based control separates and protects the integrity of executable code, according to how critical the code is to system security and operations. For example, by labeling the PCASSO code "security critical," the system prevents the corruption of code by viruses from the Internet.

What really sets PCASSO apart is its level of assurance, which the international Common Criteria for Security Evaluation defines as "ground for confidence that an entity meets its security objectives." Assurance is what makes one believe that a system will do what it is intended to do and will not do what it is not supposed to do.

Methods used in the PCASSO project to achieve high assurance include:

- **configuration management.** Sophisticated tools organize and account for all changes in the source code at the heart of PCASSO. Thus, someone who works on any of PCASSO's modules knows which source code is the most recent, who made changes, and when they were made
- **delivery and operation.** Only persons working in a privileged installer role can install PCASSO, and they must do so only from specified local computers. The label-based access controls guard against changes in security-critical applications and disclosure of sensitive patient information. PCASSO detects efforts to perform unauthorized actions
- **policy modeling.** Mathematical methods based on the Prolog language specify PCASSO's security policy to enforce discipline and maintain consistency
- **design simplicity.** Because complexity is anathema to security, all enforcement of security policy in PCASSO takes place in one software component-the server. It mediates all access and cannot be bypassed and its small size allows rigorous analysis, testing, and validation
- **least privilege.** A user or software program should be able to perform only those actions and use only those data necessary to complete assigned functions. Each active entity in PCASSO has a minimum set of capabilities; users can access only the data and applications they are specifically authorized to access
- **minimal reliance on untrusted components.** Trusted code designed for high assurance performs all of PCASSO's security enforcement. No untrusted components, such as a Web server or browser, perform important security tasks
- **software certification.** In software certification, the digital signature of a trusted certifier is attached to a file or application. The Java applet downloaded to the client is signed using SAIC's private key. PCASSO relies on its own

certificate authority to digitally sign the encryption keys issued to users, thus certifying their authenticity

- **protection commensurate with risk.** Because PCASSO is designed to provide access to highly sensitive information in the extremely hostile Internet environment, it has protective measures for countering known and anticipated threats. The server operating system incorporates all the features and assurances of a strong Internet firewall

- **safe failure.** Fail-safe techniques ensure that a breakdown of one security mechanism won't cause a breach. For example, user authentication involves multiple methods, certain security checks are redundant, and data packets never contain both the patient's data and identity

- **testing.** Tests on components and the entire system were performed throughout PCASSO's development. Every component had to prove that it did what it was intended to do. Penetration testing, also called "ethical hacking," made sure the system did not do what it was not intended to do

A Few Challenges

Initially, at least, safety came at the expense of ease of use. A substantial number of physicians complained about the multistep, challenge-response authentication and the graphical keyboard as a substitute for a real keyboard.

Also, providers did not like having their access restricted, as required by HIPAA. This runs counter to the traditional clinical computing system at UCSD and most other healthcare organizations: typically, credentialed providers can access all patient records.

In contrast, the PCASSO team has received very positive feedback from patients. That's because the Web is far superior to the old way patients gained access to their records: by requesting a photocopy. Given patients' growing concern about privacy, they appreciate PCASSO's stringent security safeguards much more than providers do.

As the PCASSO experiment continues, we will continue to work toward the goal of making health information available to patients and providers while protecting it against possible security threats. So far, we have been successful, which surely represents a step ahead for medical records systems today and in the future.

Dixie Baker *is vice president and chief technology officer for health solutions at SAIC in Redondo Beach, CA. She can be reached at Dixie.B.Baker@saic.com.*

Article citation:
Baker, Dixie B.. "PCASSO: a Model for Safe Use of the Internet in Healthcare." *Journal of AHIMA* 71, no.3 (2000): 33-36.
