Patient-Centered Access to Secure Systems Online (PCASSO): A Secure Approach to Clinical Data Access Via the World Wide Web

Daniel R. Masys, M.D. and Dixie B. Baker, Ph.D.
University of California, San Diego (UCSD) and
Science Applications International Corporation (SAIC)
La Jolla, California

The Internet's World-Wide Web (WWW) provides an appealing medium for the communication of health related information due to its ease of use and growing popularity. But current technologies for communicating data between WWW clients and servers are systematically vulnerable to certain types of security threats. Prominent among these threats are "Trojan horse" programs running on client workstations, which perform some useful and known function for a user, while breaching security via background functions that are not apparent to the user. The Patient-Centered Access to Secure Systems Online (PCASSO) project of SAIC and UCSD is a research, development and evaluation project to exploit state-of-the-art security and WWW technology for health care. PCASSO is designed to provide secure access to clinical data for healthcare providers and their patients using the Internet. PCASSO will be evaluated for both safety and effectiveness, and may provide a model for secure communications via public data networks.

INTRODUCTION

The Vision of "Internetable" Health Care

The feasibility of using the World-Wide Web (WWW) to access clinical information has been demonstrated in a number of ongoing research efforts. WWW servers and clients have been used to implement an easy-to-use Graphical User Interface to patient-specific data at a growing number of academic centers[1-5]. Though current prototypes have achieved the goal of Web access to clinical data repositories, all of them are explicitly targeted to serving only health professionals and most currently use security "firewalls" to filter queries originating from outside the organization's private network.

The full potential of a ubiquitous National Information Infrastructure (NII), however, lies in its catalysis of new and expanded opportunities for communications, not simply in the acceleration of existing lines of communication. A key theme of the NII is individual empowerment, a focus on the "customer" as a participant and partner in the flow of information. In a medical environment, this customer is the patient, who is empowered to access and control his/her own health data. Information technologies are needed that explicitly recognize the rights and responsibilities of providers and their patients and implement those rights and responsibilities via access, confidentiality, integrity, and accountability controls compatible with public data networks such as the Internet.

Elements of Information Security

Regardless of the system or information technology used, information security requires the following components[6,14]: 1) User Authentication - the assurance that a person or device is who they purport to be; 2) Access Control - the assurance that only authorized users, for authorized purposes, can gain access to a system; 3) Confidentiality - assurance that information will not be disclosed to other than authorized users under authorized circumstances; 4) Integrity - assurance that programs, data, and services are as they are expected to be , and; 5) Attribution/non-repudiation - assurance that actions taken within the system are reliably traceable. In addition, client-server models of information delivery need to accommodate the requirements of end-to-end security, which requires not only a transport channel with known security properties, but also "trusted code" on both the server and client machines to provide reliable and effective security services.

Fear of disruption of servers by hackers has received much attention in the technical and lay press, and the recent introduction of electronic commerce Web servers has brought information transport innovations such as the Secure Sockets Layer[7] (SSL), Secure HTTP[8] (SHTTP), the Secure Electronic Transactions (SET) protocol[9] and Distributed Computing Environment Web Tools (DCE Web)[10]. Protected servers and encrypted Internet communications provide only two of three necessary elements (trusted code on the server and a secured transport channel). The weakest link in the current Web is the client workstation, where commonly-used operating systems make the issue of trusted code problematic.

Specifically, commonly used PC operating systems such as Windows 3.1 and Windows 95 run in the same

1091—8280/97/$5.00

hardware and software execution domain as user applications. So neither operating system software nor any additional "trusted code" is protected from interference, corruption, or tampering. Without process isolation and hardware protection of security-critical code, the entire client environment is at risk.

Security Risks of the Current Internet

The most vexing class of security threats to Internet attached clients are "Trojan horse" programs. Trojan horses are applications that perform some useful function visible to a user, while additionally performing functions unknown to the user, which violate one of more elements of security listed above. An example would be a free downloadable Web browser program which has a unique and desirable feature, but which also covertly directs a copy of all keyboard input and files accessed to a malicious host on the Internet. Such a program could support the automated "harvesting" of credit card numbers, user account IDs and passwords, and other sensitive information in a fashion that would be essentially impossible for users to detect. Trojan horse programs are just like any other application program except for their "malicious intent" (which their creators view as "undocumented features"). Thus, like other applications, they can perform basic input/output computer operations such as file creation and keyboard input. Any program that runs in the user domain can be "Trojaned." Since common PCs run everything (operating system, communications protocols, user applications) in a single user domain, any program could be a Trojan horse.

Because of the risks inherent in Internet technology and environment, healthcare enterprises have eschewed exposing healthcare data to the Internet environment. In particular, most view the disclosure risk for highly sensitive information, such as HIV/AIDS, genetic, mental health, substance abuse, etc., as too great to bear. Trojan horses are capable of compromising the security of current web browsers, even when those browsers are operating in "secure" mode.

METHODS

PCASSO Functions

Patient-Centered Access to Secure Systems Online (PCASSO) is an architecture and implementation for providing Web-based access to sensitive clinical data. As shown in Figure 1, PCASSO is designed to provide a number of security capabilities, and a level of assurance, that go beyond what is provided by current WWW electronic commerce applications. PCASSO is currently under development under a Healthcare Information Infrastructure research contract supported by the National Library of Medicine. The key functions of the system include the following:

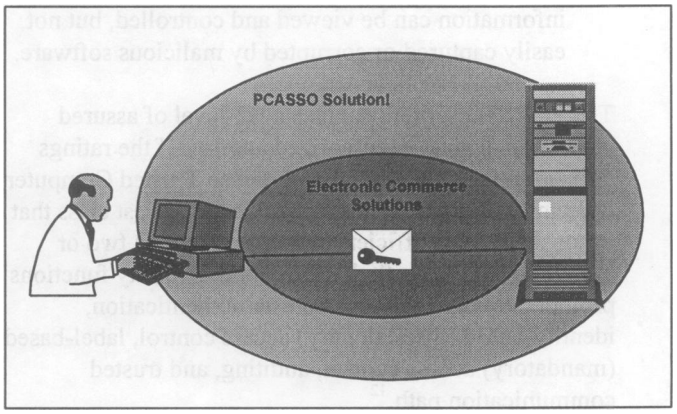

Figure 1. PCASSO provides protected server and client environments, as well as secured communications.

- PCASSO protects healthcare information at multiple levels of sensitivity, the most sensitive of which, if disclosed, could result in significant and irreversible harm to the individual (for example, mental health records and genetic information).

- PCASSO empowers consumers to "own" their own health information. Using the PCASSO system, patients will be able to access to their own health information as well as track who has accessed their health information.

- PCASSO provides an audit mechanism that records all accesses in a form that the patient can comprehend, consistent with the recently-released recommendations of the National Research Council on health information systems security[11].

- PCASSO incorporates an automated e-mail notification service, which alerts patients (and providers, if they so choose) whenever a change has occurred in their records.

- PCASSO authorizes user actions based upon their "roles" such as patient, primary caregiver, secondary caregiver, and researcher.

- PCASSO extends its security protection to the user's personal computer. As noted above, significant risks exist at the client computer, often a standard personal computer, for both unauthorized disclosure and modification. In addition, the client PC serves as the gateway into the server, so defeating client security could result in unauthorized access to the

server. To counter these risks requires that the client environment be provably trustworthy and non-corruptible. PCASSO provides a client environment in which patient-identifiable information can be viewed and controlled, but not easily captured or corrupted by malicious software.

The PCASSO server provides a B2-level of assured protection against unauthorized access. Of the ratings defined in the Department of Defense Trusted Computer System Evaluation Criteria, "B2" is the lowest class that is considered of sufficient strength to protect two or more levels of classified information. Security functions provided by class B2 include user authentication, identity-based (discretionary) access control, label-based (mandatory) access control, auditing, and trusted communication path.[12]

The strength of B2 level security comes from its inherent architectural assurances and the stringent analysis and penetration testing to which it is subjected. Because PCASSO handles patient information whose disclosure could cause grave harm to the patient, B2 is considered in the project architecture to be the minimal level of assured protection. (B2 is considered equivalent to an E4 rating according to the European Information Technology Security Evaluation Criteria.)

System Design

PCASSO integrates the security functionality of several components. Its operating system environment is Data General's DG/UX B2 Secure™. An Access Mediator program manages the roles assigned to persons registered in the system, and uses those roles to provide role-based access to a Clinical Data Repository implemented with B1-rated Trusted Oracle 7™. The Clinical Data Repository accepts HL7-formatted messages from a CAI Inc., Interface Engine which is the inter-host messaging hub of the UCSD clinical enterprise. Data are labeled by a trusted guard system as they are streamed into the secure repository, using default values for sensitivity (Non-patient-identifiable, Patient-identifiable, Public deniable, Guardian Deniable, Patient Deniable[13]) based on its source and type (e.g., HIV serology result). Web server functionality is provided by a secure customized http server that performs mutual client-server authentication using asymmetric (public-key) cryptography and session confidentiality using symmetric (private key) encryption. The client application is being implemented using Java.

Although the prototype implementation defines a specific set of sensitivity levels and user roles, and enforces a defined role-based security policy, PCASSO is designed and instrumented with the flexibility and extensibility to enable it to be used in a broad range of healthcare environments. A healthcare enterprise could define its own sensitivity levels, roles, and security policy to be enforced by PCASSO.

Phase I of the project, currently underway, includes building and testing the PCASSO system in a laboratory simulation environment. Security testing includes extensive penetration testing using a "white box" approach where system source code is available to the team attempting to breach the security.

In Phase II, to commence in late 1997, the system will be implemented in the UCSD Healthcare Network. It will first be deployed to give UCSD faculty and affiliated community physicians a Web client interface to current clinical systems. It will then be deployed to 250 volunteer patients recruited from populations of UCSD Healthcare beneficiaries who have Type I diabetes, chronic renal failure, or HIV, and who already have Internet access via an Internet Service Provider.

Evaluation

The principal questions that must be answered by the evaluation of an information access system such as PCASSO are similar to those used by the Food and Drug Administration for the introduction of any new medical technology: is it safe, and is it effective? PCASSO penetration testing will attempt to:

1. Gain access to the system without providing the required credentials or performing the required actions.
2. Read information for which the user is not authorized (including encryption keys).
3. Modify or delete information for which the simulated user is not authorized (including encryption keys).
4. Cause information to be routed to a user other than that for which it is intended.
5. Modify or delete the audit trail.

CONCLUSION

PCASSO applies state-of-the-art security technologies to the goal of extending the current World-Wide Web so that it may be used by healthcare providers and their patients to view person-identifiable health data. The project tests both the technology of security and the sociology of healthcare in an era where patients are given online access to their own medical data.

Acknowledgements

This work is supported by a Health Information Infrastructure research contract N01 LM63537-00 from the U.S. National Library of Medicine.

References

1. Cimino JJ, Socratous S, Clayton PD. "Internet as Clinical Information System: application development using the World Wide Web. J. Am. Medical Informatics Assoc. 1995: 2(5), 273-83.
2. Chute CC, Crowson DL, Buntrock JD. "Medical Information Retrieval and WWW Browsers at Mayo." In Gardner RM, ed. Proc 1995 Ann Symposium on Computer Applications in Medical Care, New Orleans, November 1995, 903-7.
3. Jagannathan V, Reddy YV, et. al. "An Overview of the CERC ARTEMIS Project." In Gardner RM, ed. Proc 1995 Ann Symposium on Computer Applications in Medical Care, New Orleans, November 1995, 12-16.
4. Kahn, CE, Bell DS. "WebSTAR: Platform-Independent Structured Reporting using World-Wide Web Technology." In Hripcsak G. ed. Proc of the 1995 Spring Congress of AMIA; Boston, MA, June 1995, 86.
5. Kohane, IS, Greenspun P, Fackler J, Szolovits P. "W3-EMRS: access to multi-institutional electronic medical records via the World Wide Web." In Hripcsak G. ed. Proc of the 1995 Spring Congress of AMIA; Boston, MA, June 1995, 86.
6. *Information Technology -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture*, ISO/IEC 7498-2, International Standards Organization, 1988.
7. Netscape Communications Corporation. The SSL Protocol. December 1994. http:// www.netscape.com/newsref/std/SSL.html
8. Rescorla, E. and Schiffman, A. The Secure HyperText Transfer Protocol. Internet Draft dated December 1994. Available as http: //www.commerce.net/cgi-bin/textit?/information /standards/drafts/shttp.txt
9. MasterCard and Visa, Secure Electronic Transaction (SET) Specification, Book 1 Business Description, Draft for public comment dated February 23, 1996. Available as http://www.mastercard.com; http://www.visa.com
10. Lewontin, S., and M. E. Zurko. "The DCE Web Project: Providing Authorization and Other Distributed Services to the World Wide Web." February 1995. http://web1.osf.org/www/dceweb/
11. For the Record: Protecting Electronic Health Information. Computer Science and Telecommunications Board. National Research Council. National Academy Press. Washington, D.C. 1997
12. Department of Defense Trusted Computer System Evaluation Criteria, DOD 5200.28-STD, December 1985.
13. Institute of Medicine, *The Computer-Based Patient Record: An Essential Technology for Health Care*, R. S. Dick and E. B. Steen, Eds., National Academy Press, Washington DC, 1991
14. Baker, DB, and Cooper, T. *Guide to Effective Health Care Information Technology Security*, in press.