Glucoweb: A Case Study of Secure, Remote Biomonitoring and Communication

Daniel J. Nigrin, M.D., M.S., Isaac S. Kohane, M.D., Ph.D.
Informatics Program and Division of Endocrinology, Children's Hospital
Boston, Massachusetts

As the Internet begins to play a greater role in many healthcare processes, it is inevitable that remote monitoring of patients' physiological parameters over the Internet will become increasingly commonplace. Internet-based communication between patients and their healthcare providers has already become prevalent, and has gained significant attention in terms of confidentiality issues. However, transmission of data directly from patients' physiological biomonitoring devices over the Web has garnered significantly less focus, especially in the area of authentication and security.

In this paper, we describe a prototype system called Glucoweb, which allows patients with diabetes mellitus to transmit their self-monitored blood glucose data directly from their personal glucometer device to their diabetes care provider over the Internet. No customized software is necessary on the patient's computer, only a Web browser and active Internet connection. We use this example to highlight key authentication and security measures that should be considered for devices that transmit healthcare data to remote locations.

INTRODUCTION

The Internet continues to grow at an accelerating pace, and it is clear that it will serve an increasingly central role in the healthcare process. In addition to acting as an information source for patients, as a means of communication between patients and their health care providers, and as an infrastructure upon which medical record systems are based, the Internet will become a part of many new and exciting medically related processes. These include telemedicine-based patient physical examinations, patient-maintained Web-based medical records, and remote monitoring of patients' physiological parameters.

With these advances, security, confidentiality, and data integrity concerns have been raised. E-mail communication between patients and their providers has already become prevalent, and best practice measures have been identified to ensure secure and confidential methods of using e-mail for this purpose[1, 2].

Less has been written in the literature about standard ways of managing the security and integrity of remotely transmitted physiological medical data, although with the rapid rise of telemedicine applications, this has begun to change in recent years[3-6]. Significantly, there has been little discussion thus far of ensuring the security of physiological monitoring devices that patients may wear or use outside of an institutional medical environment.

BACKGROUND

Remote Medical Communication

Remote communication of physiological medical data has been with us for several decades now[7]; initially, such transmission occurred over existing public telephone lines, and including such uses as remote home monitoring of patients' electrocardiograph or polysomnographic data streams[8, 9].

As network communication technologies improved, dedicated computer links between remote locales were used, including ISDN and T1 connections for applications such as remote hemodialysis monitoring and picture archiving and communications systems (PACS)[10, 11].

With these approaches, security concerns were raised, but in general have been felt to be less critical because of the one to one connection between sender and receiver. In more recent deployments of remote medical applications that use the Internet, the underlying communication framework is much more open, and issues regarding the safety and integrity of data become more paramount. Recent recommendations for a public key infrastructure[12] are helpful but lack specifics to allow implementation of ubiquitous, cost-effective and secure biomonitoring.

Remote Diabetes Mellitus Management

There is a significant body of published literature on the remote management of patients with diabetes

1067—5027/00/$5.00

mellitus. Again, the telephone was the underlying technology behind early incarnations of such systems; many of these early systems involved the transfer of glucometer data via a modem that dialed a dedicated central computer[13-16].

More recently, new approaches using the Internet have been developed, including several commercial ventures[17-20]. Some of these systems allow for direct upload of data to a central online repository; of these, some encrypt the data stream, while none authenticate the glucometer itself. Furthermore, none allow for transfer of glucometer data without additional client hardware and/or software.

DESIGN AND IMPLEMENTATION

We have developed a computer application called Glucoweb, which enables patients with diabetes mellitus to transmit their self-monitored capillary blood sugar data from their personal glucometer to their diabetes care provider(s) using secure protocols (Fig. 1). The application is written in the Java computer language, and is deployed as a Java applet. Patients do not need to have any pre-installed software on their computer apart from a Java-enabled Netscape™ Navigator browser and an active Internet connection. All that is required is a serial connection from their glucometer's data port to the serial port of their computer. This permits patients to communicate their blood glucose data while away from their home computer; for instance while at school, at work, or on vacation.

Glucoweb has been created with pediatric patients in mind, and has graphics intended to appeal to this age group. In addition to allowing patients to e-mail their blood glucose data to their physician or nurse provider, Glucoweb provides a facility for patients to append text messages (e.g. comments regarding insulin doses, meal plan, or exercise) to their blood sugar data. It also allows patients to analyze their own data within the application in a variety of different graphical and tabular formats. Glucoweb also uploads the patient's blood glucose data to a secure database, for retrieval by either patient or physician for analysis at a later time. In addition once uploaded to this central database, the glucose data is

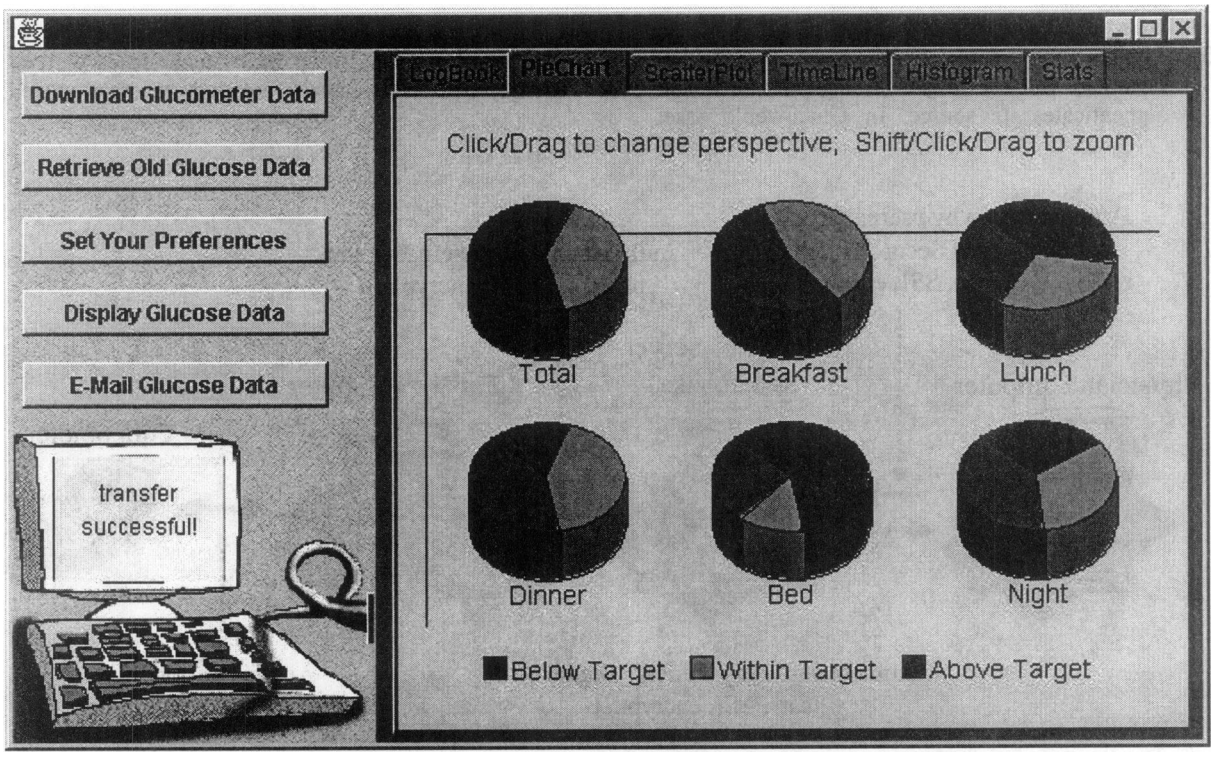

Fig.1 A sample Glucoweb screen, showing a patient's blood glucose data displayed in "Pie Chart" mode. This Java applet window is spawned from the user's standard Web browser. No special software is needed. All communication between the applet and the server is via SSL encrypted connections.

checked by a variety of algorithms to detect unusual or alarming trends; if so, the physician is notified of the occurrence.

Several authentication and security mechanisms have been implemented in Glucoweb:

1) Access to the Glucoweb web site is limited to users who have registered for the service, and who provide the correct username and password when logging onto the site. This is the minimum standard for security recommended by a national committee in 1997[21].

2) When patients register for the Glucoweb service, the serial number of their glucometer is recorded in the Glucoweb database. More than one serial number may be recorded if they have multiple glucometers. When they logon to the Glucoweb site and start the application, Glucoweb first queries the glucometer that is connected to the computer for its serial number, and checks to be sure that it matches the serial number provided by the user at registration. If not, the program will not retrieve the connected meter's stored glucose data.

3) The Glucoweb applet is a "secure" Java applet, meaning that a digitally signed certificate authenticates its source. In Glucoweb's case, VeriSign, a trusted third party certificate authority (CA), issues the certificate. There are several commercial CA's that use public key cryptography[22-24], as well as software packages that allow institutions to become their own CA. Our choice of VeriSign was only made based on prior experience and convenience.

4) Health care providers are also required to log on to the system using their own unique username and password combination. If they log in to the Glucoweb web site from a remote (i.e. outside of our institution's firewall-protected network), they are required to provide an additional password from a SecureID hardware token[25] which displays a password which changes once a minute.

5) All communication channels between the Glucoweb server and the patient and physician computers are encrypted using Secure Socket Layer encryption (SSL).

A summary of these authentication and encryption mechanisms is shown in Fig. 2.

Glucoweb has been used with a small number of patients on a testing-only basis; these trials worked sufficiently well that a prospective, randomized

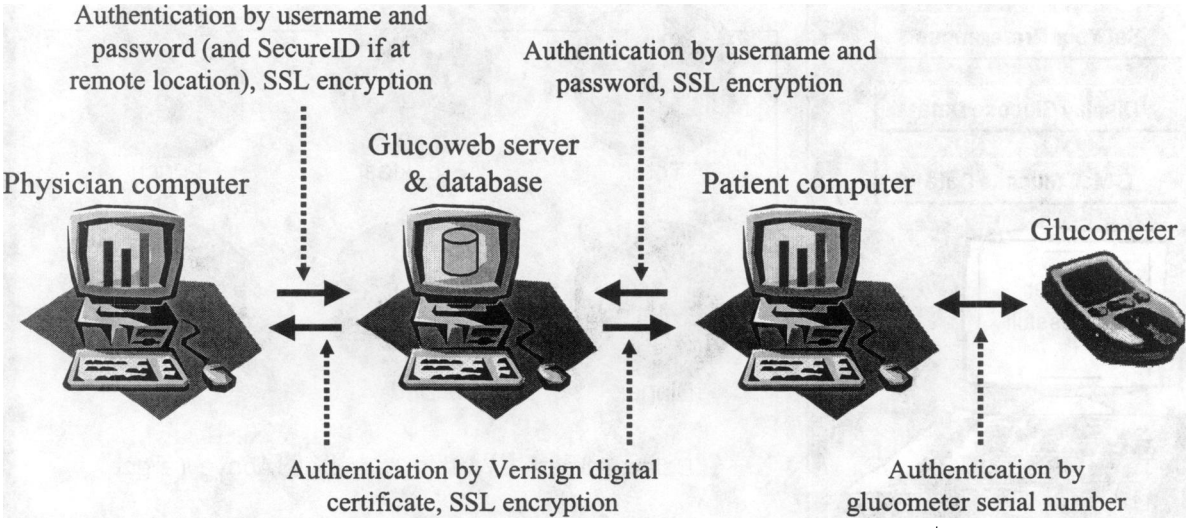

Fig. 2 A graphical depiction of the various forms of encryption and authentication used in the Glucoweb system. Unique in our approach is the inclusion of hardware-based user authentication, in the form of the patient's glucometer serial number.

clinical trial is currently in the design stages.

DISCUSSION

The security and authentication of medical data that originates from remote locations represents an important area in which significant progress remains to be made. Although the integrity of the data stream itself can be made sufficiently secure using encryption (SSL) technology, the problem of sufficiently authenticating an individual or device remains.

Several proposals have been made to create a public key infrastructure (PKI) that is either designated specifically for healthcare or is sufficiently secure for use in healthcare. Although these proposals may be directing us in the right direction, they do require significant infrastructural investments in order for their full realization. Furthermore, many of the current PKI proposals are focused on deployment of digital certificates that reside either as files on a user's computer (with all the portability and ubiquity concerns that this entails) or on a dedicated hardware token (e.g the Fortezza card[26]).

As biosensors and other patient controlled biomonitoring devices become increasingly ubiquitous, serious consideration and engineering effort should be applied to the consideration of how the data obtained through these devices should remain confidential and appropriately authenticated on its way from patient to provider. Our experience with Glucoweb suggests that a combination of multiple techniques offers the best approach.

Network security best practices often suggest a three-pronged approach to user authentication. These include ensuring that users possess:

1) Something they are
2) Something they know
3) Something they hold

The first of these implies using biometric devices to ensure that individuals are whom they claim to be. These devices are becoming increasingly reliable and less expensive, and it is certain that they will become commonplace soon. Designs for future physiologic monitoring devices could incorporate biometry for this purpose. In addition, the PKI industry may incorporate biometric devices in their future products. We did not incorporate any biometric authentication in the current version of Glucoweb, simply because our application domain did not require this level of authentication.

"Something users know" is in most cases a personal username and password. As mentioned above, this is the minimum standard for authentication and security. In most implementations of Internet-based authentication, this is the sole method used. While satisfactory for some applications, it will likely prove to be insufficient as remote medical applications are developed that deal with more sensitive data, and as more widespread use of remote biomonitoring occurs.

What individuals may "hold" is often a hardware token which uniquely identifies them. Glucoweb incorporates this form of authentication, by polling the attached glucometer for its serial number. Only when the serial number provided at the time of the patient's registration into the Glucoweb system matches that of the attached glucometer does the Glucoweb application allow access.

CONCLUSION

With Glucoweb, we have begun to approach the task of ensuring that remote patient biomonitoring data is managed in a secure and authenticated fashion. We have combined two different forms of authentication (username/password and hardware token) together with encrypted data streams. Our implementation is not perfect or exhaustive; it is only the first step in what should be more work in this field.

ACKNOWLEDGMENTS

This work has been supported in part by the National Library of Medicine (R01 LM06587-03).

REFERENCES

1. Mandl KD, Katz SB, Kohane IS. Social equity and access to the World Wide Web and E-mail: implications for design and implementation of medical applications. Proc AMIA Symp 1998:215-9.
2. Kane B, Sands DZ. Guidelines for the clinical use of electronic mail with patients. The AMIA Internet Working Group, Task Force on Guidelines for the Use of Clinic-Patient Electronic Mail. J Am Med Inform Assoc 1998;5(1):104-11.
3. Sima C, Raman R, Reddy R, Hunt W, Reddy S. Vital signs services for secure telemedicine applications. Proc AMIA Symp 1998:361-5.

4. Strauss JS, Felten CL, Okada DH, Marchevsky AM. Virtual microscopy and public-key cryptography for Internet telepathology. J Telemed Telecare 1999;5(2):105-10.
5. Wong ST. A cryptologic based trust center for medical images. J Am Med Inform Assoc 1996;3(6):410-21.
6. Makris L, Argiriou N, Strintzis MG. Network and data security design for telemedicine applications. Med Inform (Lond) 1997;22(2):133-42.
7. Goldberg E, Edery T, Desser K, Stockbridge CD, Glynn P. Remote ambulatory real time monitoring via existing public telephone circuits. J Assoc Adv Med Instrum 1971;5(4):220-3.
8. Rosekind MR, Coates TJ, Thoresen CE. Telephone transmission of all-night polysomnographic data from subjects' homes. J Nerv Ment Dis 1978;166(6):438-41.
9. Taylor KW, Liggins R, Mendler P, Schuh F. ECG telephone transmission for monitoring pacemakers and cardiac arrhythmias. Med Prog Technol 1976;4(3):133-8.
10. Agroyannis B, Fourtounas C, Romagnoli G, Skiadas M, Tsavdaris C, Chassomeris C, et al. Telemedicine technology and applications for home hemodialysis. Int J Artif Organs 1999;22(10):679-83.
11. Winchester JF, Tohme WG, Schulman KA, Collmann J, Johnson A, Meissner MC, et al. Hemodialysis patient management by telemedicine: design and implementation. Asaio J 1997;43(5):M763-6.
12. Enhancing the Internet for Medical Applications: Technical Requirements and Implementation Strategies. Washington, D.C.: National Academy Press; 2000.
13. Shultz EK, Bauman A, Hayward M, Holzman R. Improved care of patients with diabetes through telecommunications. Ann N Y Acad Sci 1992;670:141-5.
14. Gomez EJ, del Pozo F, Hernando ME. Telemedicine for diabetes care: the DIABTel approach towards diabetes telecare. Med Inform (Lond) 1996;21(4):283-95.
15. Billiard A, Rohmer V, Roques MA, Joseph MG, Suraniti S, Giraud P, et al. Telematic transmission of computerized blood glucose profiles for IDDM patients. Diabetes Care 1991;14(2):130-4.
16. Zimmet P, Lang A, Mazze RS, Endersbee R. Computer-based patient monitoring systems. Use in research and clinical practice. Diabetes Care 1988;11 Suppl 1:62-6.
17. DiabetesWell.Com, http://www.diabeteswell.com.
18. Health Hero Network, http://www.healthhero.com.
19. LifeChart, http://www.lifechart.com.
20. Metrika, http://www.metrika.com.
21. Clayton PD, Boebert WE, Defriese GH, Dowell SP, Fennell ML, Frawley KA, et al. For the Record: Protecting Electronic Health Information. Washington, D.C.: National Academy Press; 1997.
22. Kohane IS, Dong H, Szolovits P. Health information identification and de-identification toolkit. Proc AMIA Symp 1998:356-60.
23. Mjolsnes SF. Privacy, cryptographic pseudonyms and the state of health. In: Advances in cryptology; 1993; Fujiyoshida, Japan: Springer, Verlag; 1993. p. 494-.
24. Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Comm. ACM 1978;21:120-6.
25. Security Dynamics, http://www.securitydynamics.com.
26. Spyrus, http://www.spyrus.com/content/products/fortezza.