Providing Secure Access to Confidential Patient Information Detailing Diabetic Condition

Dr. D.W.Chadwick[1], Dr. J.P.New[2], Dr. D.M.McDowall[3], D.P.Mundy

Contact Author

Darren P Mundy
Email: d.mundy@salford.ac.uk
Postal: IS Institute, University of Salford, The Crescent, Salford M5 4WT
Tel No: +44 161 2955664
Fax No: +44 161 745 8169

Other Authors

[1] IS Institute, University of Salford, The Crescent, Salford M5 4WT Tel +44 161 295 5351 Fax +44 161 745 8169 Email: d.w.chadwick@salford.ac.uk
[2] Diabetes and Endocrinology, Salford Royal Hospitals NHS Trust, Hope Hospital, Stott Lane, Salford M6 8HD Tel +44 161 789 7373 ext 4625 Email: john.new@virgin.net
[3] Principal Biochemist, Salford Royal Hospitals NHS Trust, Hope Hospital, Stott Lane, Salford M6 8HD Tel +44 161 787 4970 Email: dmcdowel@fs1.ho.man.ac.uk

Abstract

Can secure access be granted to confidential patient records using the Internet? Our study has involved providing distributed access to one such confidential information database in a United Kingdom (UK) secondary care (hospital) organisation. We describe the application chosen to be distributed, the security systems used to protect the data, the reasons for the implementation decisions made and the results of the test data and feedback from the users taking part in a trial of the system.

We conclude by stating that secure access to patient information systems over the internet is possible using the architecture we have in place, but for distributed access to patient information systems to be successful the cost to ownership of the system must be far outweighed by the benefits. However, as more business processes become Internet based and high connection bandwidth becomes available at reasonable prices, systems such as ours will be present in day to day operation amongst a large number of the disparate operations of the UK National Health Service (NHS).

Keywords

Public Key Infrastructure, digital signatures, encryption, usability, validation testing

Introduction

"There are nearly 1.5 million people in the United Kingdom with diabetes, with another estimated 1.0 million people who have not yet been diagnosed. That is nearly one out of every 24 people have or could have diabetes." [1]

Secondary care organisations in the UK keep a large number of patient information databases recording information about people with chronic diseases. Most of this information is only available internally and no access is provided to NHS primary establishments. In a great number of cases [2, 3, 4, 5] though access to this information would provide more effective patient care, through a reduction in the number of duplicated investigations and also speeding up of the respective business process.

We aimed in this study to provide a secure distributed interface into a Diabetes Information System (DIS) at Hope Hospital, Salford, UK. This project was an

extension from a previous one wherein we provided secure access for General Practitioners to the DIS [6]. In this addition to that study we sought to improve the systems usability through changes to the web page format and by situating the application in an environment in which the system would prove to be of greater value to other health care workers. The health care workers which were identified as having a great deal to gain from the application were UK opticians.

Application Structure

The DIS was implemented in 1992 and holds a complete record of all the registered diabetics in the Salford area. The information stored is useful to a wide number of health specialists and with reference to ocular health the DIS stores data about diabetes related eye problems, extent of visual impairment and has a full record of patients eye history.

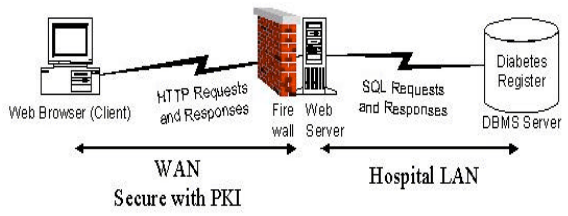

Figure 1. The Chosen Architecture

Presently opticians have no access to the data stored within the DIS either electronically or in paper format. Whenever a diabetic patient visits them they rely on their paper records from previous screenings and complete a new 3-layer carbonised paper form with the new screening details. The layers they send out to Hope Hospital for input into the DIS, to the clients GP and the bottom sheet they keep for their own records. It then takes a number of months for the information received by Hope Hospital to be input into the DIS because of the large volume of results received.

The DIS is situated on the trusted hospital Intranet and therefore no data security is in place. To make the database externally accessible over the Internet however a security structure needs to be provided (Figure 1) because of the fact that the Internet is a highly insecure network for transfer of important or confidential information [7].

The backbone behind our secure network solution to the information transfer is a Public Key Infrastructure (PKI). This provides the needed requisites of encryption and authentication so we can be sure that data is secure in transit (encryption) and only authorised users are allowed access (authentication). The PKI we have used has been provided by Entrust [8] this decision was made purely on the basis of previous implementations and familiarity. A Checkpoint [9] firewall is in place at the hospital to prevent undesirable users from accessing the hospitals trusted network.

Our system operates via the transmission of HyperText Transmission Protocol (HTTP) requests over a private channel through the firewall to a web server on the hospital Local Area Network (LAN). The HTTP requests are transformed into Structured Query Language (SQL) requests for information from the DIS. The information is then routed back to the client PC and displayed in HyperText Markup Language (HTML) format. The web session is secured via the use of a secure proxy server and client application. All information transferred over the channel is encrypted and digitally signed using the users private signing key. If the user is authenticated they are allowed access through the firewall and to the DIS.

Implementation

After analysis of the feedback generated from the previous interface to the DIS we identified a number of improvements needed to make this extension a success. These are identified in summary below:

Performance of web-site – we were required to optimise the interface size and speed up the access over a dial up connection. The content required was a reduced subset of the previous GP interface therefore the application had a lower amount of data to retrieve via SQL statements from the DIS. However, the extra functionality required by the users resulted in a larger page to download.

Format of page – We had found previously that medical professionals disliked having to scroll down a web page to view patient information. Therefore a decision was taken to transform the interface into a multi-tab formatted page (Figure 2) with the use of HTML layering to control the visibility of particular HTML areas on the form.

Usefulness of system – Opticians have expressed an interest in having the access to the DIS in place. In the previous trial the person to get the most out of the access was a consultant ophthalmologist. Therefore we believed that the system would be beneficial to the opticians in the hospital's surrounding area.

System reliability – Poor network performance was apparent in the previous system trials, just 93% availability. We believe that this had a dramatic affect on user perception of our system. Salford Universities network infrastructure has undergone major improvements and we believed that this would make a positive impact on system availability and therefore user perception.

PKI Installation – Installation problems had been a major problem in the past but we hoped that with the arrival of a new version of our security software these problems would disappear. A decision had also been made to abandon the need for smart card access to our interface because of previous poor performance [10] especially in the amount of time required for installation.

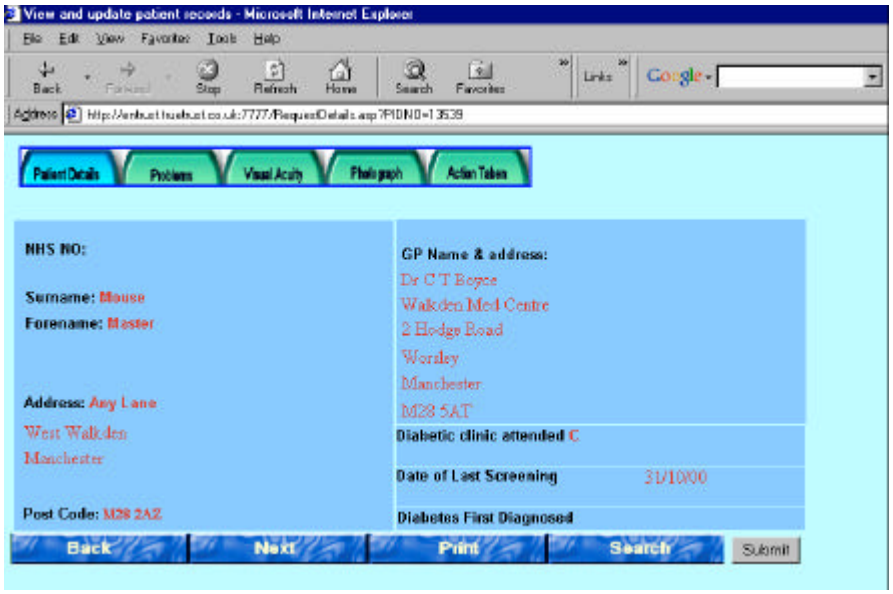

Figure 2 The Interface Design

Validation Testing

After the interface had been upgraded but before installation in the user environment, we carried out a series of validation checks. These tests took between ten and fifteen minutes to complete and within each series of test scenarios we aimed to test the following:

- Secure logon to the application
- Search and retrieval of a patient records
- Update patient information in DIS
- Logout and closedown of the application
- Attempted insecure logon to the application

Test Category	Required Performance	Actual Performance
User Testing	42 tests allocated to testers	42 tests attempted 2 tests completely aborted 36 tests completed and considered analysable
Overall First Time Success Rate	99%	75% (FAIL)
PKI Functionality		
User Installation	99% within 15 minutes	100% (PASS)
User Revocation	100% success	100% (PASS)
User Re-Installation	100% success	100% (PASS)
Hardware Components Availability		
NT4 workstation running LDAP directory	99% availability	100% (PASS)
NT4 PC running Entrust CA infrastructure	99% availability	100% (PASS)
Database server running diabetic register	99% availability	100% (PASS)
Network Uptime	99% availability	98.36% average (FAIL)
Software Components Availability		
LDAP directory server	99% availability	75% availability (FAIL)
Entrust CA server	99% availability	75% availability (FAIL)
Entrust Direct Server Proxy	99% availability	60% availability (FAIL)
IIS server + Scripts	99% availability	100% (PASS)
Data		
Integrity	100% accurate	100% accurate (PASS)
Ease of use and Performance		
Time spent to learn to use the system	Less than 15 minutes	Between 0 and 8 minutes (PASS)
Time to launch the application after connection to the Internet has been opened	Less than 60 seconds	Between 20 and 60 seconds (PASS)
Time spent to initiate a request	Less than 30 seconds	Less than 1.5 minutes for the combined operation (PASS)
Time for reply to be received	Less than 1 minute	
Keying errors/mistakes in use	<1%	<1% (PASS)

Table 1. The Validation Test Results

We also tested network availability over the validation testing and user trial period. The results of the validation tests are displayed in Table 1.

Test Results

A team of eight validation checkers carried out a total of forty two tests on the interface. Only three of the eight testers had not been installed as an Entrust user previously. Each of the new installations though succeeded in the fifteen minutes we had set as an allowable time for system integration. Overall we attribute this installation improvement from the previous project to the new version of software we have obtained from Entrust. The components required for our system to operate are now shipped on a single CD rather than the dual CD format we used previously.

The first time test results did not meet expectations with a 75% success rate. This could be attributed to user errors when performing the tests, problems with the test data itself and more importantly a couple of failures in the interface itself.

One of the failures was a consequence of two testers trying to access the interface at the same time. For the validation tests everyone used the same username and password. The interface for security reasons will not allow multiple logins using the same account details, consequently the system logged out user A when user B logged into the system. When user A tried to perform another operation the system displayed a security error. The other failure was a SQL timeout error. This error may reoccur when opticians are using the system owing to performance issues and heavy usage of the DIS by users.

Administration errors caused poor availability of both the Certificate Authority (CA) and Lightweight Directory Access Protocol (LDAP) servers. The errors were a result of upgrading our security infrastructure and we are confident that they would not happen repeatedly. The network availability has now increased to 98% but this is still below the 99% availability we would expect in a modern environment.

User Pilots and Feedback

Three opticians across different sites were found for a one-month trial of the application. All had a PC in place and in two cases a linked digital camera. A user request made by the opticians which we incorporated into the interface, involved the secure transmission of patient optical retinal images to the hospital.

Installation

A number of browser configuration problems were experienced both in the installation process and on completed install.
Conflict with Internet Service provider (ISP) Proxy server – involved simple installation and set-up of a different ISP package.
Corrupted browser installation – solved by re-installation of the Internet browser.
Display of large fonts – needed to reduce the font size within the web browser. This unfortunately is a poor solution and font display should have been considered at an earlier stage.

All of the problems were easy to resolve and involved no significant time loss. At the end of the trial period we carried out an interview with each of the opticians to ascertain their views on the following areas:

Reasons for joining the trial

The main goal of the trialists was that the trial would lead to the provision of a better client service to their diabetic patients. By taking part in the trial they believed that they could contribute to the development of the interface and better enable the system to meet their expectations.

Comment on present system and assess benefits of electronic access

All were generally dissatisfied with the present paper based record system but

recognised the fact that it was familiar. Criticised was the delivery method of the form via the postal service and its overall complexity. A proportion of the current paper is perceived to be irrelevant.

Electronic access it is felt would have a large number of benefits and as long as the system is implemented well, with few problems. The most important benefit that the opticians believed would come from electronic access is the optimisation of the complete business process.

Usability of the system

Although the opticians were impressed with the general layout of the interface screens, over the time of the trial they formed the opinion that they would rather scroll down a web page than have to click between tabs. This is the opposite opinion to the feedback we had received previously from the GPs.

Time to access the application again was a major issue. In a trial situation where users are only using the interface for short time periods each day this is a definite problem. The main issue is that the initial ISP and Entrust logon period is greater than forty seconds from dial in. The users simply were not prepared to wait this long before they could gain access to a patient's record. After the connection has been established however the whole experience becomes less time consuming. This problem will only be solved by installing a permanent Internet connection in the optician's shops, so that Internet access will be immediate.

Problems experienced when using the system

During the trial we had a number of problems with ensuring 100% system reliability. For a number of days the system was down owing to problems with Hope Hospital's firewall and the secure proxy server. Also the users experienced problems with forgotten passwords and out of date information on the DIS. In the current paper based system it can take several months for data to be input into the DIS. Therefore on some occasions the optician's records were more up to date than the computer system.

All of these factors contributed to a general feeling that the system was unreliable from a connection point of view and also in its data integrity. Of course this problem will disappear once an online system becomes permanently operational, but during the pilot this clearly was not the case.

Evaluation of usage and future usage

The interface was used sparingly during the trial. The speed and connection problems caused varying amounts of frustration and the opticians could not afford to spend a large amount of time within the system. The outlook for future adaptation was however good with each of the opticians stating that they would continue to use the system once operational, as long as improvements could be made to the access time and the reliability of the data.

Attitudes to data security

The users showed little concern for the overall system security and they hardly noticed that high security was in place. The opticians accepted that the environment was secure when transacting with the hospital. No questions were raised about the actual processes behind the interface and the opticians showed complete trust in the implementation team. As the system had been recommended to the opticians by consultants in the hospital they felt they could trust the security in place.

Conclusions

With the addition of a web interface and secure infrastructure, we have shown that it is possible to extend the operation and usefulness of existing legacy applications within the NHS. It is also apparent that

these systems can be distributed over the insecure public network without the loss of privacy of information as long as data is encrypted and users are authenticated.

We have found slow Internet connection time to be a significant impediment to the widespread adoption of systems such as ours. The main problem is the dial up connection to the ISP. When the system is in use for only short periods the overhead of the connection is too long for the users to accept. All of the opticians have however asked to keep the system in place because there are benefits to their use of it.

User interface design is extremely difficult to get right. What is right for one set of users is often fundamentally wrong for others. We have had negative feedback about both layouts of the interface that we have tried. However, if the interface had been updated then placed back with the opticians we feel that they would have been happy that their feedback had been accepted and satisfied with the system layout.

We conclude that for the short periods that the system is used at present, the cost to benefit ratio is perceived as being too great. However, with the cost of broadband access ever decreasing and a national plan to have permanent connections to the NHSnet [11] installed in primary care establishments we feel that systems like the one we have implemented will eventually become widespread in practice.

References

[1] http://www.diabetic.org.uk/diabetes-insight.htm, Diabetes Insight, 24th January 2001

[2] HealthCare Informatics, HealthCare Takes the e-Train, http://www.healthcare-informatics.com/issues/1999/09_99/cover.htm September 1999

[3] Engelbrecht, R. Hildebrand, C., DiabCard, http://www-mi.gsf.de/diabcard/

[4] Raghupathi, W. (1997) ‘Health care information systems’, *Communications of the ACM* 40, 8: 81-82.

[5] Neumann, P.J., Parente, S.T. and Paramore, L.C. (1996) ‘Potential savings from using information technology applications in health care in the United States’, *International Journal of Technology Assessment in Health Care*, 12(3), 425-435.

[6] Chadwick, D. W., Cook, P.J., Young, A.J., McDowell, D.M. and New, J.P. 2000, 'Using the Internet to Access Confidential Patient Records: A Case Study', British Medical Journal, vol. 321, pp. 612-614.

[7] Hawkins, S., Yen, D.C., Chou, D.C. “Awareness and challenges of Internet security”, Information Management and Computer Security, 8/3 [2000], 133-143

[8] see http://www.entrust.com

[9] see http://www.checkpoint.com

[10] Chadwick, D. W. 1999, 'Smart Cards Aren't Always the Smart Choice', IEEE Computer, vol. 32, no. 12, pp. 142-143.

[11] Department of Health. Information for health: an information strategy for the modern NHS 1998-2005. www.nhsia.nhs.uk/strategy/full/index.htm