CONCEPT FOR INCREASED SECURITY FOR INTERNET/INTRANET - BASED ADMINISTRATION OF PATIENT DATA

Lutz Vorwerk, Sergey Khludov, Christoph Meinel

Department of Telemedicine
Institute of Telematics, Bahnhofstraße 30-32
54292 Trier
Germany
vorwerk@ti.fhg.de www.ti.fhg.de

ABSTRACT

In this paper, we will present an increased-security concept for systems administering patient-data and DICOM (digital imaging and communication in medicine) images. The system presented here is an intranet/internet-based PACS and has been developed at the institute of telematics (IT) [Hlu99]. The PACS is based on standard network-protocols and has been created using DICOM – standard. See [Nem94] and [Rad99] for more information. The system components have been designed in JAVA and have been distributed onto three different computers. Two computers - equipped with several relational databases administered by JAVA servers - were assigned to the intranet-component while the third computer is located on the internet and is equipped with an user interface. The concept for increased security developed at the IT aims at protecting the intranet against the internet. Interaction between the components on the internet and within the intranet should take place via a secure connection. Patient data can either be sent encoded along with images or can be sent separately from the raw image data. System users are entered into and administered by an user database. A standard "registry" will act as the user database, allowing users to access data.

Keywords: Internet, Intranet, PACS, Firewall, SSL, LDAP, Registry, WWW, JAVA, DICOM

1. INTRODUCTION

Applications that are based on an intranet and/or on the internet offer a broad range of possibilities for communication and data-visualisation. Several exemplary applications used on the WWW have shown that it is possible, with little effort, to generate systems that are both user-friendly, potent and support communication.

Existing library classifications can be used for the simple implementation of data-input and for the data-visualisation of image data. Using JAVA-technology, already existing computer hardware (PCs, Macintosh-computers and workstations) with different operating systems can easily be integrated into the system. To allow this integration, only two conditions must be met: one, a JAVA-runtime environment (JRE) for the operating system in use and two, a browser with integrated JAVA-support. In this context, this paper examines a JAVA-based, intranet/internet-orientated transmission- and visualisation system for medical images. Users of intra- or internet may use this system to access medical images stored in the database or stored locally and allows them to use several DICOM-modalities.

2. PRESENTATION OF THE SYSTEM

Figure 1 [Hlu99] on next page shows the internet/intranet information system for transferring and editing DICOM data. The system consists of 5 basic components:

- the DICOM-database and the DICOM-archive (computer 1),
- the web server and the DICOM database (computer 2),
- the client internet browser (computer 3),
- user administration and

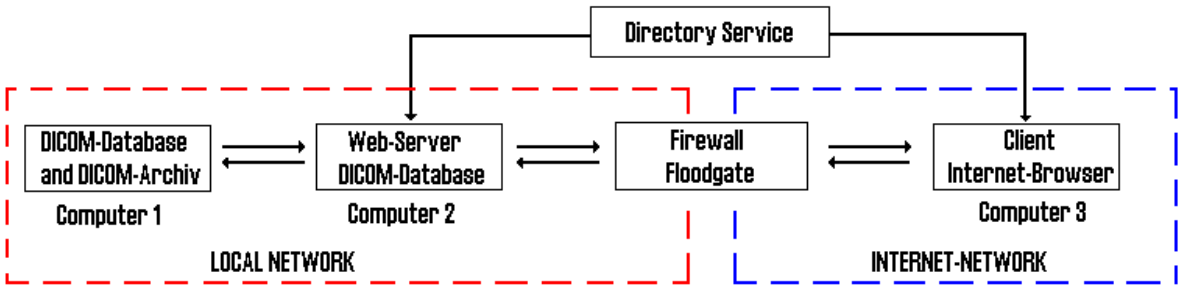

Figure 1
Structure of the internet/intranet information system for the transfer of DICOM data

- a mechanism for increased security that imitates the lock principle (to ward of external attacking)

The DICOM data is located on computer 1 and partly on the DICOM database on computer 2. The JAVA servers are installed on both computers, thus realising links with relational DICOM databases. A web server, a JAVA application and program-logic (servlet classes, applet classes, JAVA development kit (JDK), JAVA servlet development kit (JSDK), JAVA database connectivity (JDBC) and hypertext mark-up language (HTML) page) are also installed on computer 2. An internet browser is installed on the client computer. The client administration represented as a directory service is responsible for safe transmission of the codes from the server to the client. Figure 2 on next page shows the data-exchange between the components of this system.

In its internet browser, the client displays the internet address (URL = uniform resource locator) of the medical institution's internet/intranet information system, thus calling up the first HTML page. The user is now being asked to enter login and password. Servlet 1 checks the entered values. In case the authentication was unsuccessful, a new HTML page 2 for the user's personal information is created by one of the servlets. After the data has been checked, the user receives a personal login, password, and code for the codification of the DICOM data from the user administration. This data as well as the user's personal data is being saved by servlet 2 on the database for personal data. After successful authentication servlet 1 generates HTML page 3 in order to indicate the parameters of the DICOM images needed which have to be searched for in the DICOM database. Next, servlet 3 is started by using HTML page 3 and the search parameters are transferred to the servlet. Servlet 3 starts client JAVA application 1 which passes the search parameters onto JAVA server 1 (computer 2) and to JAVA server 2 (computer 1). Both JAVA servers are searching the required information through the SQL-interface on the DICOM database and in the DICOM file system. The data found is transmitted to the client JAVA application by the JAVA server, thus creating file 1 with this data on hard disc of computer 2. Servlet 3 then creates HTML page 4 to call up a DICOM viewer applet (DAV). The DAV reads file 1, then logs it into the internet browser of the client (computer 3). To view the scaled version of the DICOM image or the original image the user has to press the button `JPEG Preview` or the button `View original image` or `View condensed image`.

In this case, the DAV starts HTML page 5. The user states the name of the image and starts servlet 4. Servlet 4 starts the client JAVA application 2 and copies the name of the file. Client JAVA application 2 analyses file 1 and determines - based on the image name - the computer and the directory where the image is stored and copies it onto the hard disc of computer 2 as file 2. Servlet 4 then creates the next HTML page 6 which calls up the DBV applet. The DBV applet reads file 2 and logs it into the internet browser of the user (computer 3). The information in the PAV applet chart can be viewed by the user only after being decoded. Analogously, the client should decode the image in the DBV applet.

3. CONCEPT FOR INCREASED SECURITY IN PATIENT DATABASES

The patient database - developed and implemented at the institute of telematics - call for login in by the physician as a first step (shown by figure 2 on next page). This procedure - a nuisance to physicians who have to use this system on a daily basis - can be substituted by an authentication process through certification. This way of entering the system requires a trustworthy authority (certificate authority (CA)) to edit the certificates and pass them to the users. Whenever a directory service is employed for user administration, already existing properties can be used for safe transmission of passwords.

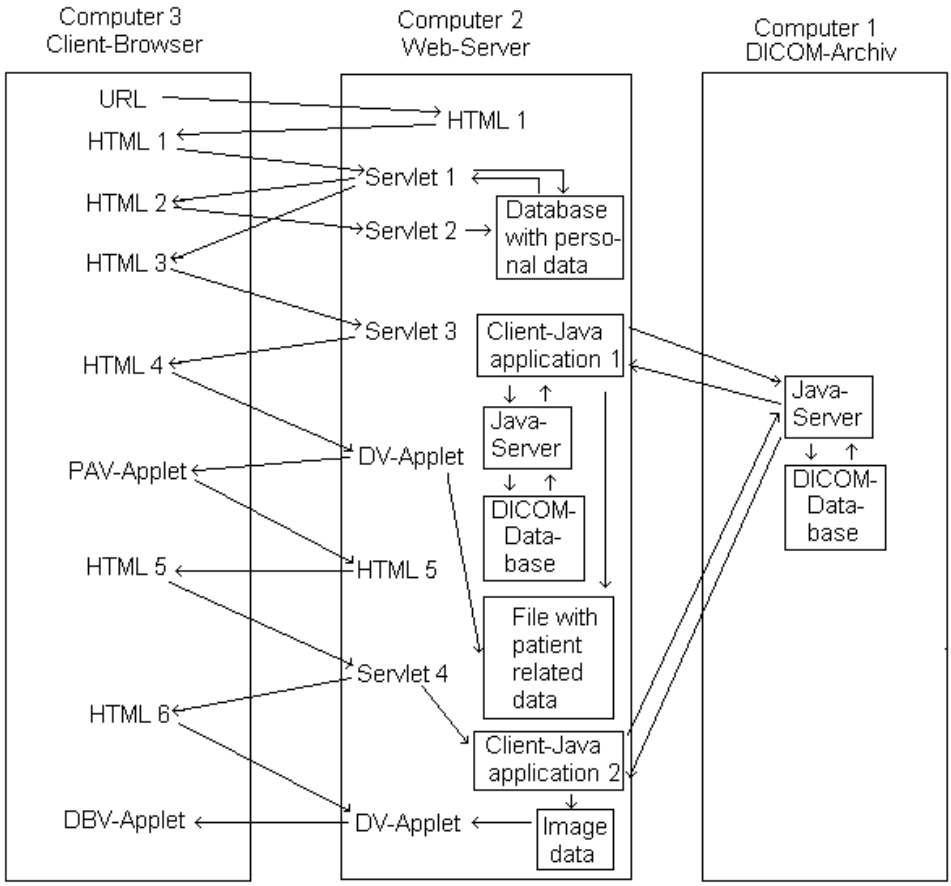

Figure 2
Structure of data exchange between the components of the internet/intranet information system for the transmission and the handling of DICOM data

To establish a SSL (secure socket layer) link to the client, the directory service uses certificates issued by a trustworthy authority. This protocol must be assigned to the International Standard Organisation – Open System Interconnection (ISO-OSI) basic reference model of the security level. By making use of the ´handshake´ method, the SSL-protocol determines which version of the protocol and which type of codification to use.

4. USING THE DIRECTORY SERVICE FOR USER ADMINISTRATION

The lightweight directory access protocol (LDAP) has furthered the idea of using browsers as a basis for administrative tasks. LDAP is based on the direct access protocol (DAP) which, in turn, is a simplification of the standard X.500 [Alo99]. By adding the standard X.509-based SSL [Net96], [Hou99]), security between client and server can be guaranteed. Any person wishing to be identified through personal login and password has to apply for a certificate at a certificate authority (CA).

Communication between server and client via SSL proceeds as follows: The server sends a certificate to the client together with a public key. At the CA, the client verifies the certificate and begins - if the identification was successful - with the transfer of the data codified by the public key. The server decodes the incoming data with its private key. Next, in order to get identified by the directory service, the client sends off its certificate.

The access rights of successfully identified clients are predefined (reading, writing). When being identified, the client “slips” into the “role” of administrator, physician or medical technical assistant (MTA). The certificate of the client contains a public key as well.

When the certificate of the authenticating directory service user has been accepted, the user may use the directory service at the appropriate access level without re-entering the password and login. This process is called “single sign on”. Here, Netscape Suite Spot is used for the administration

of LDAP, SSL and for certification mechanisms. In this package, the personnel of the directory service and the administration of the certificate-server is carried out by directory administration.

All certificates of people, directory servers and certificate servers contain the distinguished name (dn) of their owner. This dn is needed for the hierarchical classification of the registered servers or of the registered personnel. It is composed of the node identifier in the directory tree. The dn determines the role of the certificate owner.

To transform a JAVA stand-alone application into an applet, security management of the Netscape Communicator 4.05 in Solaris 2.51 must be taken into consideration. The security management asks for the use of the java4.0 jar library and for signing the JAVA-applet.

The library-classification is a component of Netscape Communicators. In order to sign the JAVA applet, the operating system must contain Netscape's signtool [Net99b].

Alternatively, Smartupdate [Net99a] can be used. Smartupdate is restricted to Windows 9x and Windows NT though and was not used therefore. However, there is a possibility of escaping the security mechanism (in case connections between different computers need to be tested) by supplementing one of the Netscape configuration files.

Using Netscape Communicator's security mechanisms has an effect on the management of the SLAP (stand alone LDAP database) [Uni96] which contains personal data. A link to the directory server is established via SSL by the applet code and the HTML-implementation of JAVA script.

If client and server have successfully exchanged certificates and certificates have been checked and accepted, a SSL-link is established, coding the ensuing interaction between client and directory server.

Thus, important patient data can be exchanged without the danger of third parties "listening in" and filtering information from the data flow.

Inner attacks can be prevented in logging every action that may violates the system. If the directory service is properly configured in setting access rights, the modification of files so that third persons gain access to the system can be prevented by logging and assigning access rights to data or functionality. Additionally, all components used have to be digitally signed to prevent the possibility of modification.

There are other methods of realising an authentication. One of it is Kerberos. This system enables a good prevention of packet sniffing and impersonation but adds complexity to administrate the system [Atk96]. We used a directory service in order to implement security as an asymmetric architecture that uses digitally signed public keys with information about the owner of the assigned private key (certificates) instead of tokens that carry information about the access rights to specific functionality. The method using a directory service is more efficient in verifying if a user is permitted to use specific functionality of the system.

The next section shows how a directory service is working and describes its advantages in user management.

5. THE DIRECTORY SERVICE AS PART OF THE INCREASED SECURITY CONCEPT

In the next step, we aim to "depict" the user administration in the directory service so that we will be able to differentiate between doctors and MTAs so that access rights to patient data may be classified. The major concern of DICOM is patient management. Physicians can be assigned to patients. These references are depicted as a model in the directory service.

Corresponding attributes of the DICOM document files such as information about the physician-in-charge may be read. If there are no values assigned to these attributes, the administrator will be asked to which physician the documents should be assigned.

Next, in the directory service, objects are being generated, establishing a reference to the medical data in the directory service and to the DICOM document. This concept can be enriched, later on, by adding options for the checking of access rights (adding to and changing attribute entries in DICOM-documents).

After the physician has received the patient's data, the transfer of image data is initiated. In this case, the images concerned are not DICOM images but scaled images compressed as a format developed by the Joint Photographic Experts Group (JPEG). Thus, a preview becomes possible. These pieces of data do not need extra protection when transmitted since they cannot be assigned to any specific patient.

Once an image from the preview has been chosen for processing, the server transmits the original DICOM image. It must be taken into consideration here that patient information is transmitted together with the image.

Thus, in this case, secure transmission of data is vital. If the headers (DICOM documents) of the DICOM images are being administered in the directory service, secure transmission is ensured by using a SSL-link.

The data can be separated into image data and DICOM document data. DICOM document data is administered in the directory service and is linked to the image data (still being stored on a file system) via a reference connection.

Thus, image data can be safely transmitted without needing to be encoded and patient data as well as data needed for the visualisation of an image can be transmitted via an encoded link.

The DICOM protocol is not necessary for the intranet component of the patient database since the elements of this component should not be replaced. For dealing with the outer, image-producing modalities, the DICOM protocol must be used since it configures the intranet components to the interaction of image-producing modality. It is sufficient to create a basis for a DICOM-protocol which supports the properties needed by the patient database. This basis can be expanded later on.

It is necessary, though, to integrate security aspects into the DICOM-protocol. The transport layer security (TLS) support feature will be added (according to the standard it will be added as ´handshake`). Using foreign applications provided by the DICOM-protocol does not make much sense since such applications are not defined for patient database properties.

Contacting externally located internet components requires taking extra steps to protect the intranet. One possibility to do so would be firewalls. However, firewalls are not very useful for transmitting documents. Much rather, they are fit for making interaction of users via the internet possible. The alternative solution is a firewall-principle which allows a separation of internet and intranet while transmitting data. This concept has been evaluated in banking and is now one of the components being integrated into PACS. Its predominant feature is, in particular, an easier configuration than that of firewalls.

6. CONCLUSION

Easier and faster transmission of medical data between hospitals and practising physicians is becoming increasingly important which results in a growing demand for internet and intranet applications. Since unauthorised access to information about patients must be prevented, it is important that data transmission be extremely safe. In this paper, we suggested SSL for secure transmission and as a defence mechanism for attacks located externally (i.e. on the internet) we proposed the early-called ` floodgates´ [Haf98] now renamed in `lock keeper´, a concept developed at the IT. Even for authorised users, access rights must be assigned, determining which data may be accessed by which user. A directory service based on a LDAP-protocol was the right choice for the administration of legitimate access. Signing the components of the system prevents from modification in order to allow third persons to gain access to the system.

7. REFERENCES:

[Ali99] Computer Networks Destinations Home, *Aloni Systems*, X.500, Request for Comments Documents (RFCs), http://www.aloni.com/CND/CNDest.asp?TOCId=IPFamily&TopicID=X500, 1997-1999, (last visit November 99)

[Hou99] R. Houseley W.Ford, Spyrus, VeriSign, W. Polk, NIST, D. Solo, Citicorp, Internet X.509 Public Key, Infrastructure, Certificate and CRL Profile, http://www.cis.ohio-state.edu/htbin/rfc/rfc2459.html, January 99, (last visit November 99)

[Net99a] SmartUpdate, Netscape Communications Corporation,http://home.netscape.com/smartupdate/su1_30.html, 1999, (last visit November 99)

[Net99b] Signing Software with Netscape Signing Tool 1.1, Netscape Communications Corporation, http://developer.netscape.com/docs/manuals/signedobj/signtool/index.htm, 1999, (last visit November 99)

[Uni96] The SLAPD and SLURPD Administrators Guide, University of Michigan, Release 3.3, http://www.secretagent.com/groupware/sldap-doc/1.html#RTFToC1, April 30, 1996, (last visit November 99)

[Net96] Netscape Communications Corporation, Netscape Products security, SSL 3.0 SPECIFICATION,http://home.netscape.com/eng/ssl3/3-SPEC.HTM#2, 1996, (last visit November 99)

[Haf98] E.G. Haffner, Thomas Engel, Christoph Meinel, *Floodgates statt Firewall Eine High Security –Lösung zum sicheren Daten-austausch zwischen Internet und Intranet*, 1998

[Rad99] *Radiology*, PennState College of Medicine, http://www.xray.hmc.psu.edu/dicom/dicom_home.html, 1999, (last visit November 99)

[Nem94] NEMA Standard Publication PS3.X: *Digital Image and Communications in Medicine*, Parts 1-10, 1994

[Hlu99] S. Hludov, L. Vorwerk, Ch. Meinel.: *Intranet/Internet-basierte PACS*. Teleme-dizinführer Deutschland – Ausgabe 2000 (ISBN 3-0000-4589-9) , 250-253, 1999.

[Atk96] D. Atkins, P. Buis, C. Hare, R. Kelly, C. Nachenberg, A. B. Nelson, P. Phillips, Tim Ritchey, W. Stean, *Internet Security*, News Readers, 1996