SECURITY INFRASTRUCTURE FOR ELECTRONIC ARCHIVE USING OPEN SOURCE SOFTWARE

Radek Doležel
Doctoral Degree Programme (1), FEEC BUT
E-mail: xdolez35@stud.feec.vutbr.cz

Supervised by: Václav Zeman
E-mail: zeman@feec.vutbr.cz

ABSTRACT

The paper describes the design of security infrastructure for electronic archive protection, its installation and configuration. The designed infrastructure is based on an open source software solution, which uses the Debian GNU/Linux operating system and services powered by the Alfresco, Apache Tomcat, OpenLDAP and OpenSSL projects. In the paper, main strengths and weaknesses that occurred during the work, are also assessed.

1 INTRODUCTION

A great number of services in computer networks are based on a client and server model. The connection established between a client and a server is not secured in most cases. If secret data are transmitted from the server to client's computer, it is necessary to protect the connection between these two points. For this reason it is suitable to build the whole new infrastructure, because also other services take part in the secured connection.

This paper reflects some parts of author's Master thesis, *Design of security infrastructure for electronic archive* [1], which includes more details of the following description.

The open source software has been selected for the design and building of this infrastructure, in particular the Debian GNU/Linux [2] operating system and the Alfresco [3], Apache Tomcat [4], OpenLDAP [5] and OpenSSL [6] projects as the appropriate services.

2 DESIGN OF SECURITY INFRASTRUCTURE

The infrastructure is based on the client and server model. This model, which describes the whole infrastructure, is in Figure 1. The infrastructure consists of several parts, but the two main components are server-01 and pc-01, which are situated in a private network. The private network is separated from the Internet by a device that includes a router and a switch. The listings of the software and the certificates are shown below server-01 and pc-01. We used the private network for a proper installation and configuration of the software, and for a laboratory validation of security.

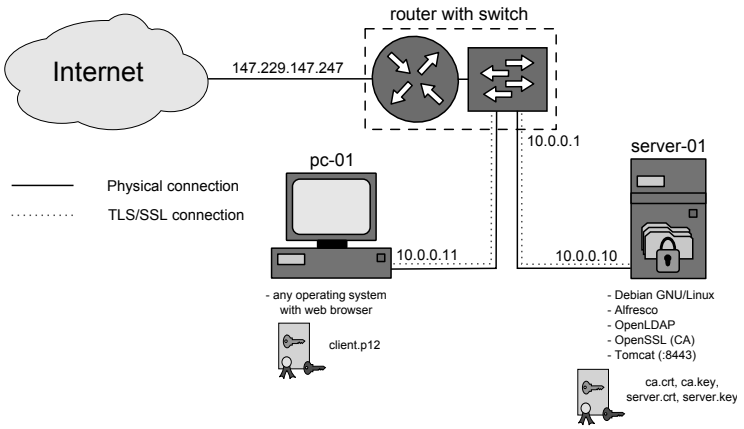

Figure 1: Design of security infrastructure.

- *server-01* represents an electronic archive that provides services. The installed and configured software is the Alfresco, Apache Tomcat, OpenLDAP, OpenSSL projects and the Debian GNU/Linux operating system.
- *pc-01* is client's personal computer, which is independent on the platform of an operating system. A web browser compatible with certificates is required.

3 INSTALLATION OF SERVER SOFTWARE

The Debian GNU/Linux operating system was installed as the base on server-01. The command line version of installation is sufficient. After the installation of the operating system and its basic configuration the software was installed. The installation procedure is not dependent on the installation sequence of subsequent software, but the installation of Alfresco alone requires to install Apache Tomcat first. In most cases Alfresco is installed together with Apache Tomcat. Next, OpenLDAP and OpenSSL could be installed.

4 CONFIGURATION OF SERVER SOFTWARE

If the installation of software was successful, then it is necessary to configure the appropriate services, because each of these services is dependent on the others.

4.1 OPENSSL

The whole infrastructure of a certification authority was built using the OpenSSL project. The certification authority generates the self-signed certificates with the matching keys for server-01 and pc-01. For pc-01 (client) the certificate with the matching key in one file was issued. It is protected by the PIN (Personal Identification Number). These certificates with the matching keys are used to establish the secured connection between server-01 and pc-01.

4.2 OPENLDAP

The user profile items are stored in an OpenLDAP data structure. This structure is outlined in Figure 2 and it is in a very simplified version that could be expanded. Figure 2 shows

two user groups. The first group called Administration is for the administrative work and the management of Alfresco. The second one is Users and it includes common users for a routine work in Alfresco. Each user profile could be filled with a variety of parameters such as real name, login name, password, email address, organization's name, etc. Data could be inserted directly one by one into the directory structure, but for our import a template file was written. The password of every imported user profile is encrypted.

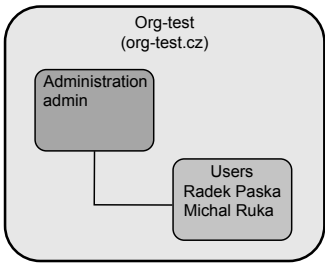

Figure 2: Structure of user data in OpenLDAP.

4.3 ALFRESCO

Alfresco uses its own database for user profile items in original installation. The configuration of authentication and synchronization forced Alfresco to use the OpenLDAP data structure. In the authentication part, information about authentication and network connection to OpenLDAP were set up. The items for the synchronization and their synchronization period were set up in the part of the synchronization.

4.4 APACHE TOMCAT

Apache Tomcat offers an unsecured connection via common HTTP (Hypertext Transfer Protocol) and secured connection with certificates via HTTPS (Hypertext Transfer Protocol Secure). The usage of the secured variant requires the import of the server certificate with the matching key into the key storage of Apache Tomcat. The properties of the connection were set up after the import. That is represented by the enabling of the secure mode, change of the connection port and system path to the key storage, set up of the password for the key storage and selection of the mode of client authentication. In general cases authentication of the server alone is used, i.e. only the client validates the server certificate. Mutual authentication is most secure, because the server as well as the client are authenticated. This scenario was selected, because the certification authority issued the certificate with the matching key for both server-01 and pc-01 (client). It is also possible to provide the mixed version when the unsecured and secured connection is used.

5 CONFIGURATION OF CLIENT SOFTWARE

Mutual authentication requires the storing of the client certificate into client's key storage. The web browser has its own key storage. The client certificate could be imported into the secured storage of the web browser, but a hardware cryptographic token or a smart card could be also used as the storage.

6 SUMMARY OF SOFTWARE STRUCTURE AND USER INTERFACE

The summary of the designed infrastructure from the software point of view is shown in Figure 3. The figure is divided into quadrants, where the horizontal axis represents the ISO/OSI layer model, precisely the application layer and other lower layers. The vertical axis includes the client and server model on each side.

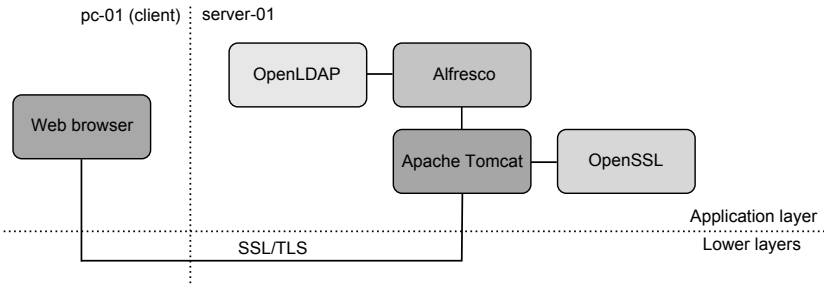

Figure 3: Software structure.

The user web interface is in Figure 4. The synchronized items of the user profile called *radek.paska* and secured connection via HTTPS are shown there.

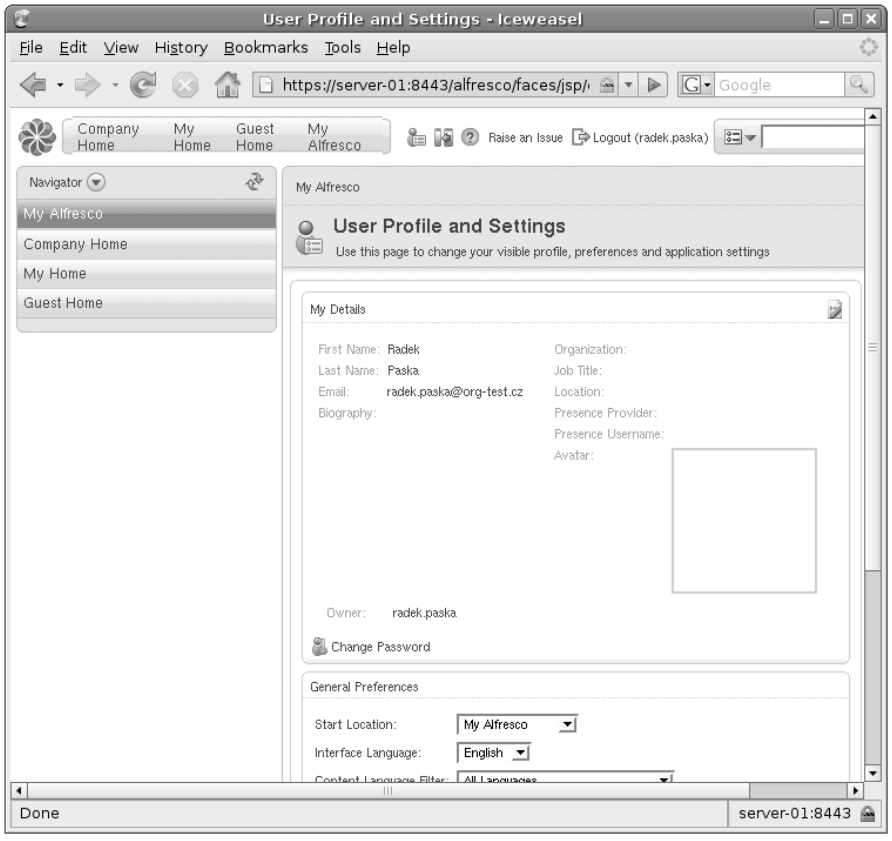

Figure 4: User web interface for *radek.paska*.

7 CONCLUSION

The article describes the design and building of the security infrastructure for protecting the electronic archive. The designed infrastructure is based on the client and server model and consists of two main parts. The first part is the server-01 electronic archive with appropriate services and the second one is client's computer pc-01, which uses the services provided by server-01. The software for the electronic archive is certain called Alfresco. Apache Tomcat is used for creating the web interface with mutual authentication (server and client). A weakness, that occurred during the configuration of Apache Tomcat, was the plain text password of the key storage in a configuration file. The services of OpenSSL are used for the secured connection. OpenSSL represents the whole certification authority, which generates the self-signed certificates. The weakness of OpenSSL was the storing of the root certificate with the matching key of the certification authority in a common directory. To avoid the danger of secret data compromise it is suitable to restrict user access rights. The user profile items of Alfresco are stored in OpenLDAP data structure. According to the synchronization of Alfresco with OpenLDAP, Alfresco is authenticated to OpenLDAP first and then data are synchronized. In this point we found the two weaknesses. The first weakness was the plain text authentication password in a configuration file. The second one was the one-way synchronization, i.e. from OpenLDAP to Alfresco. The user profile items could be changed only in OpenLDAP. The client certificate was stored for the validation of the mutual authentication into the secured storage of the web browser first and then it was stored in the hardware cryptographic token.

The main strengths are the usage of an open source software solution and the independence on the platform of the operating system. Some weaknesses were discovered during the configuration and validation of the whole infrastructure. It is possible that the weaknesses are amended in the new versions of the software implementations.

REFERENCES

[1] DOLEŽEL R. *Design of security infrastructure for electronic archive* (in Czech). Brno: Brno University of Technology, The Faculty of Electrical Engineering and Communication, 2009. 106 p. Supervisor of Master's thesis doc. Ing. Václav Zeman, Ph.D.

[2] *Debian – The Universal Operating System* [online]. 1997 – 2010, last update 23. 2. 2010 [cit. 2010-03-01]. Available: <http://www.debian.org/>.

[3] *Open Source Enterprise Content Management System (CMS) by Alfresco* [online]. 2010, [cit. 2010-03-01]. Available: <http://www.alfresco.com/>.

[4] *Apache Tomcat* [online]. 1999 – 2010, [cit. 2010-03-01]. Available: <http://tomcat.apache.org/>.

[5] *OpenLDAP* [online]. 2010, last update 10. 6. 2009 [cit. 2010-03-01]. Available: <http://www.openldap.org/>.

[6] *OpenSSL: The Open Source toolkit for SSL/TLS* [online]. 1999 – 2009, [cit. 2010-03-01]. Available: <http://www.openssl.org/>.