The Authentication Techniques in Distributed E-Learning between Universities in Avicenna Virtual Campus Network

Amjad Mahfouth
Information Technology, Alquds Open University
Tulkarm,09,Palestine

Abstract

E-Learning become the most used and popular teaching method in universities with availability of E-learning tools and techniques, development of technology communications and networks. In this paper we will propose authentication techniques between universities in Avicenna Virtual Campus Project in Euro Mid Infrastructure Network.

These universities are sharing a resources to support the E-learning System between them, since the universities are usually isolated graphically in the world. The system are in a risk and dangerous from hacking, viruses and un trusted peoples.

The security issue is very important for the thousands of students, employees and instructors whom access the E-learning resources and translate data between universities network.

Keywords: *E-learning, Security, Authentication, MyProxy, Certificates.*

1. Introduction

In Avicenna Virtual Campus Project, is one example of distributed system, the resources and data are distributed on long areas, large scale, different area and different people whom access the resource in the system, so the Administrators are looking for security to maintain the system from hacking, viruses, Trojan horse, spam and un trusted people access the resources in a system. There are some components of security technique like Authentications, Authorizations, Data Encryption and Proxy Credentials. In this paper we propose a security for Avicenna Virtual Campus Project that address the requirement for single sign on, interoperability with local policy and dynamic resources.

Authentication i s important to authorization, confidentiality and access resources, if authentication fails, the whole System security will fail [1][3]. Authentication is
needed because users, companies, resources are shared and distributed on large areas.

2. What is the problem?

As you see from the figure 1, the Avicenna virtual campus project, which is a group of twenty university distributed on the Middle East and Europe, distributed on large areas, different areas and different people will access the resource in scalable system. The Management of security in this system is very complex and very important issue because the characteristics of the systems are dynamic and large number of distributed resource and users. The dynamic nature of this system can make it impossible to establish trust relationships between places when the students and lecturers login to the resources to access the lectures, schedule, exams, doing experiments, access library , translate data and sharing resources between them.

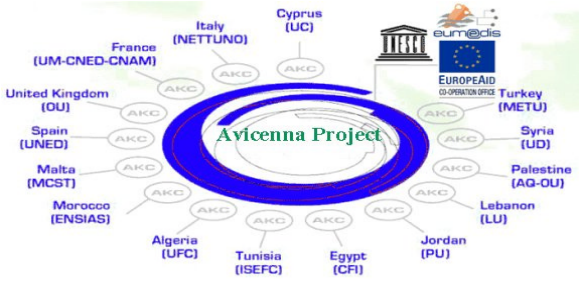

Figure 1, Avicenna Virtual Campus Project[6]

3. Avicenna Virtual Campus

Avicenna Virtual Campus[6] is an ambitious project that aims at creating new community of universities sharing best practices and pedagogical innovation through a network of E-learning centers across the Mediterranean. It involves 15 countries including Palestine which is represented by AL-Quds Open University (QOU), to realize one of its important objectives, E-Learning has become a key part of QOU development strategy. The project is dedicated to accelerating the adoption and best use of ICT-assisted Open Distance Learning (ODL)

in 11 Mediterranean non-EU Member States. Demand for ODL in the target Universities and societies already exist. The project aims at establishing adequate local infrastructures and to transfer best practice and professional know-how within target universities. The project is named after Ibn Sina (981-1037 Ad) the most famous philosopher of his time

4. System Security Mechanism

The proposed Authentication techniques consist of the following security sub section.

4.1 Public Key Infrastructure (PKI)

PKI [3] is recognized as an essential enabling technology for security in a large scale network. The main in PKI is Certificate. A Certificate is a data structure containing the public key and related details about the key owner and signed by a Certification Authority (CA). The role of the certificate is to bind the public key to a particular entity on the system. The private key represents the identity of each entity on the system[3].
PKI[3] used in Cryptography in sending data messages through channel, the Public key cryptography (asymmetric encryption), each party has a pair of related keys: one for encryption and one for decryption. The same key cannot be used for both. The main assumption in public key cryptography is that one of the keys must remain secret (private key) and the other is made public (public key). The main assumption in public key cryptography is that the Private Key must remain secret. One way to protect the private key file is to encrypt it with a password. So, if it is stolen, the user will have enough time to revoke his corresponding public key [3].

4.2 Digital Certificates

Digital certificates are digital documents that associate a network resource with its specific public key. A certificate is a data structure containing a public key and Pertinent details about the key owner[3]. A certificate is considered to be a tamper proof electronic ID when it signed by the Certification Authority for the system environment. Digital certificates, also called X.509 certificates, act very much like passports, it provides a means of identifying network resources between universities [2][3]. The important fact to know and understand about digital certificates is that the
CA certifies that the enclosed public key belong to the entity listed in the certificate.

When a system client[3] wants to start a session with a system recipient, he or she does not attach the public key to the message, but the certificate instead. The recipient receives the communication with the certificate and then checks the signature of the Certificate Authority within the certificate. If the signature was signed by a certifier that he or she trusts, the recipient can safely accept that the public key contained in the certificate is really from the sender. This prevents someone from using a fraudulent public key to impersonate the public key owner. The digital certificate contains information about you and your public key. When you communicate with another party on the network, the recipient will use your public key (contained in your digital certificate) to decrypt the SSL session ID, which is used to encrypt all data transferred between network computers[3],

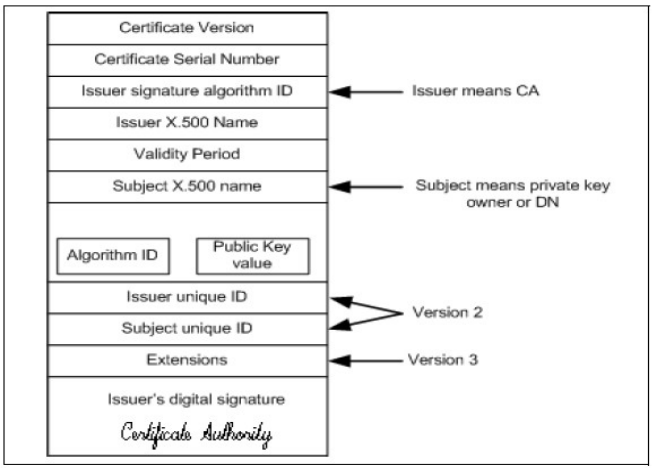

Figure 2: Digital Certificate [3]

4.3 The Certificate Authority

A CA [3] is an institution trusted by others to guarantee for the authenticity of a public key. The main role of the CA is to issue digital certificates that cryptographically bind a public key to the user's identity information. This is done by signing the information using the CA's private key. The relying parties
require the CA's public key so that they can verify the digital signature on the certificates issued by the CA .
The CA is responsible for approving or rejecting requests for the certificate of public keys and responsibility of validating that the user's information is correct before the signed digital certificate is sent back to the user. Before a CA can sign and issue certificates for others, it has to do the same thing to itself so that its identity can be represented by its own certificate.

4.4 MyProxy

Myproxy [4] is an online credential trusted server, used to store and manage user credentials, private keys and certificates. In addition the server can be used to perform delegation on user's behalf. When the user logs in, he creates a proxy certificate and sends it to the MyProxy server along with a tag and a pass phrase. When the user initiates a job request from portal or a program, the process running the job connects to the MyProxy server, presents the tag and the pass phrase, and receives a proxy for that user. The advantages of introducing this server are [3]:

• There is no need to generate the key pairs on users' machine.
• Protect the user's private key
• Provide mobility for users so they don't have to carry their private key on a floppy or their mailbox.

4.5 Authentication

Authentication and Authorization allow a network resource to identify who is requesting access to the resource and if they are allowed to use the resource. Authenticating a request is the usually first step in getting access to a network resource [4].

5. Case Study "Security Techniques in Avicenna Virtual Campus Project between Universities "

5.1 Introduction

In this section we will discuss the security in distributed E-learning between universities in Avicenna virtual campus project, figure 1.

With the development of communication and networks technology, high bandwidth, real time transmission, high equality of video and audio. E-learning become the most used and popular teaching method on a universities.

Now there is work to build e-learning network between these universities to share course material, video conference, live course, libraries, technical reports, simulation experiments in Lab., see lectures, media lecture, sharing between students and instructor's interaction and exchanging information between universities.

In this case we will show how to maintain and secure the resources between universities with a large number of students, professors, resources and apply the authentication technique that allow student to access the resources in secure channel, and provide the communication channel and authentication protocol.

5.2 Why Avicenna project?

As we said before, there are very large number of sharing resources, large number of students and instructors are distributed on large geographical areas.

The management of security issue is very important to save the users, resources and data when access and translate data in a system. since the AlQuds Open University is a member of Avicenna Virtual Campus Network. .

5.3 System Portal Interface

A System portal is a web server that provides an interface with necessary software to communicate to system services and resources, allowing students to submit compute jobs, transfer files, access lectures, login and access the system resources in Avicenna virtual campus project.

5.4 Portal Accounts

Every student have an id which is a registration numbers in a university and special a password which take it from registration department. The student can log in through portal of university like http://ritaj.birzeit.edu or http://portal.qou.edu. To check with schedule courses, grades, course registrations, marks, access library, see lectures, exams and so on.

5.5 MyProxy and System Portals

MyProxy provides a solution for delegating credentials to system portals to allow the portal to authenticate to system services on the user's behalf. Once you've stored a credential on the MyProxy server, you can "login" to the system portal with your MyProxy username and pass phrase in figure 3. If the system portal supports multiple MyProxy servers, you will also need to indicate which MyProxy server you're using on the portal login page[5]. Once you login, you should be able to use the system portal interface to access system services and resources.

The system portal takes the MyProxy username and pass phrase entered by the user and uses them to authenticate to the MyProxy server to retrieve a credential.

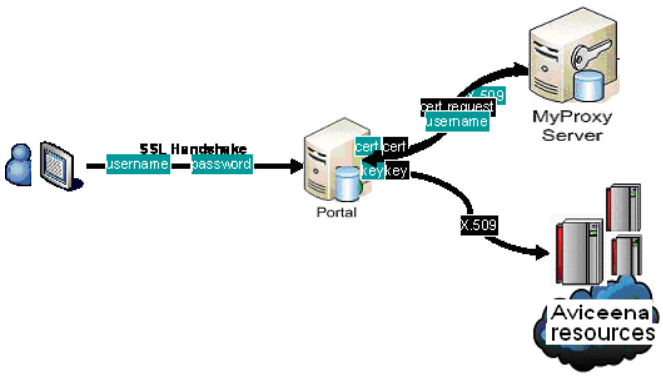

Figure 3 , Authentication processes for access Avicenna Virtual campus resources

5.6 Access resources in Avicenna Campus project

In order to guarantee a secure access to the system resources, there are multi layer security in system figure 3, all web transactions and authentication protocol are executed under the Secure Socket Layer (SSL) via HTTPS.

The students have an account on the User Interface in system portal, when a user login the system, authentication is based on the concept of user credentials delegation implemented with MyProxy. The user can using the private key of his X.509 personal certificate to create a temporary certificate issuer (a MyProxy) and store it for amount of time on a MyProxy Server. When the user asks the system portal to invoke a system resource, the portal contacts the MyProxy Server and tries to get a temporary proxy certificate on the user's behalf from the certificate issuer, if the life time of the MyProxy is not expired, temporary user credentials are retrieved, the action is performed and the output is back into the user's web browser. The objective of My Proxy's credentials delegation are to avoid the private key of the user's certificate to be sent over the network avoiding a security risk.

When the student's wants to use specific course resource, the subject of his certificate is verified against the one stored in the users server of the corresponding course resource service and if the check is successful the user can invoke the specific resource.

When a user logs into the application, the application obtains a proxy certificate from the MyProxy service using the user's ID/password, and the application can then use this proxy to authenticate to any other course resource .

The benefits of this algorithm technique are:

- Users never have to see or manage their system credentials.
- The MyProxy service is store users credentials which can be retrieved from web portal interfaces
- The registration service, user credentials, and MyProxy service can be re-used in other applications in the system.

7. Conclusion

In this paper we proposed a new authentication technique algorithm to safe the system users and system resources from hacking. We apply the authentication process in Avicenna virtual campus project between universities, when users access the e-learning resources by certifications, my proxy server and user credentials, since the system is dynamic, scalable and large number of users and resources.

After this research the reader should know the Authentication technique which is used in a system and the component parts of the Authentication technique which is the most important in Security.

We discuss an application example of distributed system, Provide a security is more difficult in system due to scalability, dynamically, large number of distributed users and resources. Every student and resources should have a certificate to identify him self on a system, from trusted Certificate Authority. Every student has a proxy certificate which is stored in MyProxy server to protect the certificate from a risk and a void the need to re enter the user pass phrase and reduce the exposure of user private key, the web transactions and authentication protocol are executed under the Secure Socket Layer (SSL) via HTTPS.

Future Work:

In the next generation we expect the development of security as follows:

- Provide long life time proxy certificate in my proxy server
- Provide more power security technique in access resource.
- provide password for a group of student upon courses

References

[1] Alexander Kemalov, *A Security Policy in GRID Architecture : International Conference on Computer Systems and Technologies - CompSysTech' 2005* , *sasho*@hsi.iccs.bas.bg

[2] Randy Butler and Von Welch .”A National-Scale Authentication Infrastructure, ”Proc. IEEE Symp. Research in Security and Privacy, December 2000.

[3] Bart Jacob,Michael Brown, Kentaro Fukui and Nihar Trivedi, *Introduction to Grid Computing.* International Technical Support Organization: Redbooks, December,2005. Available: http://ibm.com/redbooks. [Accessed Nov. , 2010].

[4] Ali Nasrat Haidar, "Critical Evaluation of Current Approaches to Grid Security," M.S. thesis, University of London,Royal Holloawy,London, 2002-2003.

[5] Weijia jia,Wanlei Zhou, Title: *Distributed network Systems from Concept to Implementation.* Springer Science: Business Media,2005. Available: http://ebooks.springerlink.com.

[6] http://avicenna.qou.edu/. [Accessed January, 2012]

Amjad Mahfouth: B.S in Computer Sciencse / Alquds University-Palestine 1998**.** Mc.S. in Scientific Computing from Birzeit University,2006. Academic Super Visor at Information Technology College in Alquds Open University. I had Worked as a Computers Technician lab. In Aquds Open University. Teacher Assistant in Computer Science In Birzeit University. Interested in Networking and Security.