Graduate Program in Information Science and Telecommunications and Networking
School of Information Sciences
University of Pittsburgh

TEL2821/IS2150: INTRODUCTION TO SECURITY

Lab 4: PKI Certificate Management

Version 1.2, Last Edited: November 19, 2007

Contact:
Saubhagya Joshi
{srjoshi at mail.sis.pitt.edu}

Group Members: ____

____

____

____

Date of Experiment: ____

Graduate Program in Information Science and Telecommunications and Networking
School of Information Sciences
University of Pittsburgh

Part I: Objective

The objective of this laboratory exercise is as follows:

1 Building a simple, illustrative PKI structure.
2 Certificate Management for PKI using Microsoft Windows components.
3 Deploying https layer on a website.
4 Creating and using Certificate Revocation Lists.

In this lab session you are expected to learn about deploying PKI using Microsoft Windows components. You are expected to work the three key components: *root certificate authority*, *subordinate certificate authority* and *client certificate requesters*. The PKI deployment over websites will demonstrate secure connection between client and server using both server authentication and client authentication.

Introduction to PKI

Why PKI

More and more organizations are moving towards a web-presence and conducting businesses online. Therefore legislative as well as regulatory requirements are becoming prominent, for example, the Government Paperwork Elimination Act (GPEA) and the Health Insurance Portability and Accountability Act (HIPAA). There is need for a mechanism to provide the information security assurances demanded by the regulations.

In order to address the security requirements the basic issues should be identified: *data integrity*, *confidentiality*, *non-repudiation* and *identification & authentication*. Data integrity services protect against unauthorized or accidental modification of data. Confidentiality services ensure that only authorized individuals have access to restricted content. Identification and authentication services validate the origin of data and its transmission. Non-repudiation services prevent an individual from denying previous access to data. Various mechanisms, both cryptographic as well as non-cryptographic mechanisms are available to address the security issues.

Cryptographic mechanisms include *symmetric key*, *secure hash*, and *asymmetric-key* (public key) mechanism. An example of symmetric key mechanisms is Advanced Encryption Standard (AES), which provide strong confidentiality and some level of integrity using message authentication code (MAC). However this mechanism does not provide non-repudiation services and needs a trusted third party for key distribution. An example of secure hash algorithms is Hash-based Message Authentication Code (HMAC), which is used to ensure integrity of data. However, confidentiality and non-repudiation services are not provided. Asymmetric key mechanisms integrate the best of the other mechanisms and cater to all of the basic security requirements by using different algorithms: *digital signature* algorithms, *key transport* and *key agreement*. Digital signature algorithms (like RSA and DSA) along with encryption algorithms (like AES) provide authentication, non-repudiation and confidentiality. On the other hand, key agreement algorithms like Diffie-Hellman provide asymmetric key exchange mechanism. Key transport mechanism can be accomplished by using strong encryption algorithm like RSA as the example below illustrates.

Example of Key Transport mechanism

Let us say *Alice* wants to send a message to *Bob* have to use asymmetric key mechanism. Each owns a pair of keys: *private* key and a *public* key. Any data encrypted using a *private* key can be decrypted using a *public* key and vice versa. *Alice* generates an AES key to encrypt the message, called a cipher. She encrypts the shared key with *Bob*'s public key, and sends both the encrypted message and encrypted key to *Bob*. *Bob* can then obtain the AES key by using his *private* key and then decrypt the AES cipher.

What is PKI

The Public Key Infrastructure (PKI) ensures that the information assurance is maintained by providing security services. The infrastructure provides a framework in which individuals can build and maintain trust relationships. The main components of PKI are Certification Authorities (CA), Registration Authorities (RA), PKI Certificates, Certificate Revocation List (CRL) and PKI Users. CAs issue Certificates to users after they have verified their credentials with the RA. Revocations of previously issued certificates are published as CRLs. Certificates denote trust relationships with the CA. Depending upon the requirements enterprise PKI architectures can be either hierarchical or mesh infrastructure.

Certificates, *CRL*s and *attribute certificates* (AC) are data structures of PKI. Certificates contain the information about the user, the public key, information about issuer, issuer's signature, purpose of certificate, its validity, other policy information and other certificate extensions. CRL is a list of revoked certificates with the issuer's signature. Attribute certificates are used to provide additional information about the user, especially where trust levels are based on not only the identity but other attributes like membership of a role, or, other contextual information. However, operational costs for short-lived AC are high. In addition to basic security services, PKI also provide services for key recovery and authorization.

Introduction to HTTPS and SSL

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) is a communication protocol that employs a normal HTTP protocol and secure socket layer (SSL) sub-layer to enable secure connection between client and secure web-server. The protocol was first used by Netscape Communications Corporation to provide authentication and encrypted communication. SSL is an open, nonproprietary protocol that Netscape has proposed as a standard to the World Wide Consortium (W3C).

HTTPS and SSL support the use of X.509 digital certificates from the server, which means that the client can authenticate a server. The limitation of HTTPS is that it is infeasible to use name-based virtual hosting with HTTPS. This is because the secure layer operates below HTTP and therefore the server can provide only one certificate for a particular IP/port combination.

Part II: Equipment/Software

Two servers are available for the lab: (i) Windows Server 2003 (WinSrv2003), and, (ii) Windows Small Business Server 2003 (SBS2003). The access accounts and passwords are given on the screen. The two machines can talk to each other directly.

You will require familiarity with the following applications:

Windows Management consoles:

- IIS Management Console
- Certificate Manager

Internet Browsers:

- Internet Explorer 7 Browser
- Firefox 2.x Browser

Installation CD for Windows 2003 Server

- Evaluation version

Part III: Exercises

You can do the following exercises either in laboratory in the Windows 2003 server machines, or re-create the exercise environment in any other Windows 2000 server (or later) environment of your choice. In order to enable other students to do the lab conveniently, please rollback the system to its original state. The guidelines for rollback are provided in Part IV: Appendix A.

Scenario

In this exercise you are the Chief Security Officer for a newly established web-based business. You are planning to create an intermediate certificate authority (subordinateCA) within your organization, which is in turn certified by a root certificate authority (CA) as shown in Figure 1. You want to restrict access to Webserver2 to authenticated users within the PKI structure.

The one-directional arrows denote who issues the certificate. For example the SubordinateCA is issued a certificate by the CA. The bi-directional arrows denote authentication between parties.

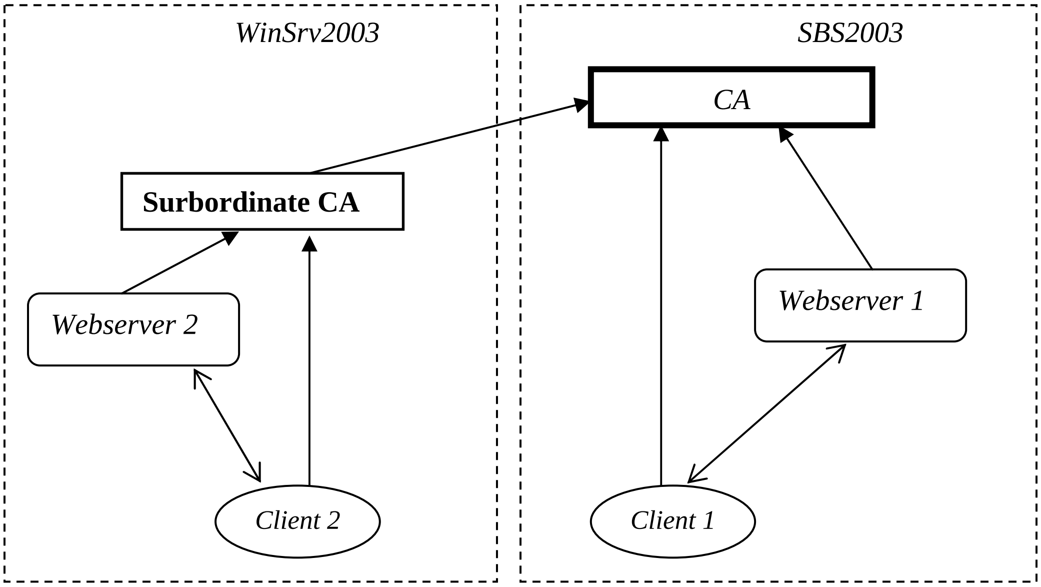

Figure 1. Architecture using PKI

Exercise 1: Establishing the Standalone CA and subordinate CA

<u>*Objective*</u>

The objective of this exercise is to establish the root CA and the intermediate CA.

<u>*Steps*</u>

To install a stand-alone root certification authority **(on SBS2003)**

1 Log on to the system as administrative user “lab4” (password: “sis.sec.lab.123”).

2 From the Control Panel open the **Add or Remove Programs** and then **Add/Remove Windows Components**.
3 In the Windows Components Wizard, select the **Certificate Services** check box. A dialog box appears to inform you that the computer cannot be renamed and that the computer cannot be joined to or removed from a domain after Certificate Services is installed. Click **yes**, and then click **next**.
4 Click Stand-alone root CA.
5 Type the common name of the certification authority. None of this information can be changed after the CA setup is complete.
6 In Validity period, specify the validity duration for the root CA. You can accept default setting of 5 years. Click **Next**.
7 Specify the storage locations of the certificate database, the certificate database log, and the shared folder. Click **Next**.
8 If Internet Information Services (IIS) is running, you will receive a request to stop the service before proceeding with the installation. Click **OK**.
9 When prompted, type the path to the Certificate Services installation files. The Windows 2003 Server installation CD is provided. Alternatively, you can also point to the folder “C:/I386” for the required installation files.

Install a stand-alone subordinate certification authority **(on WinSrv2003)**

1 Similar to the root certificate authority in SBS2003, open the **Add/Remove Windows Components**.
2 In the Windows Components Wizard, select the **Certificate Services** check box. A dialog box appears to inform you that the computer cannot be renamed and that the computer cannot be joined to or removed from a domain after Certificate Services is installed. Click **yes**, and then click **next**.
3 Click Stand-alone subordinate CA.
4 Type the common name of the certification authority. None of this information can be changed after the CA setup is complete. Click **Next**.
5 Specify the storage locations of the certificate database, the certificate database log, and the shared folder. Click **Next**.
6 Obtain the certificate for the subordinate CA. You can use either methods given below:
   a. Click Send the request directly to a CA already on the network. In Computer Name, type the name of the computer on which the parent CA is installed. In Parent CA, click the name of the parent CA.
   b. Save the certificate request as file and transport the file to the CA. This can be done using ftp service, or, by using an external storage media (like flash drive, floppy, etc.)
7 If Internet Information Services (IIS) is running, you will receive a request to stop the service before proceeding with the installation. Click **OK**.
8 If prompted, type the path to the Certificate Services installation files.
9 In the Parent CA’s **certification authority**, issue the pending certificate.
10 Export the newly issued certificate to a file.
11 Load the file into subordinate’s **certification authority** and start service.

<u>*Questions*</u>

1 Now that you have the root CA and the intermediate CA defined, what is the next step in building the PKI infrastructure? Explain briefly.
(……………………………………………………………………………………)
(……………………………………………………………………………………)
(……………………………………………………………………………………)

2 Who do you think takes on the role of the RA?
(……………………………………………………………………………….)

Exercise 2: Certificate Requests and Issuing Certificates

Objective

The objective of this exercise is to be able to generate certificate requests and issue or deny certificate requests to PKI users.

Description

Similar to the issuance of certificates to subordinate CA, certificate requests must be made by the clients to the CA within their domain. According to the scenario described above, the client 1 sends certificate request to subordinate CA and client 2 sends certificate request to root CA.

Steps

To request a certificate from a stand-alone CA or stand-alone subordinate CA

1 Log on to the computer where you want to install a certificate.
2 Start Internet Explorer, and connect to the computer hosting Certificate Services (for example, http://<servername>/certsrv).
3 On the Microsoft Certificate Services Welcome page, click Request a certificate.
4 On the Request a Certificate page, click Web Browser Certificate.
5 Fill out the information and click **Submit**.
6 If a **Potential Security Violation** dialog box is displayed, click **Yes**.
7 After the **Certificate Pending** page displays, close the browser.

To approve the pending certificate request

1 Log on to the computer hosting Certificate Services as a Certification Authority Administrator.
2 On the Windows desktop, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Certification Authority**.
3 In **Certification Authority**, expand the node for your certification authority name, and then click **Pending Requests**.
4 In the results pane, right-click the pending request from the previous procedure, point to **All Tasks**, and then click **Issue**.
5 Click **Issued Certificates**, and confirm the certificate you just issued is listed.
6 Close Certification Authority.

To retrieve the certificate

1 Log on to the computer where you want to install a certificate; for example, Gateway Server or Management Server.
2 Start Internet Explorer, and then connect to the computer hosting Certificate Services (for example, http://<servername>/certsrv).
3 On the Microsoft Certificate Services Welcome page, click View the status of a pending certificate request.
4 On the **View the Status of a Pending Certificate Request** page, click the certificate you requested.
5 On the Certificate Issued page, click Install this certificate.
6 In the Potential Scripting Violation dialog box, click Yes.

7 On the Certificate Installed page, after you see the message that Your new certificate has been successfully installed, close the browser.

Questions

1 When the PKI user creates the certificate request, there is a warning message saying that the user should continue only if the server is trusted. What is the significance of this warning?
(……………………………………………………………………………………)
(……………………………………………………………………………………)
(……………………………………………………………………………………)

Exercise 3: Establishing a secure web by deploying HTTPS

Objectives

1 Deploy a web server with HTTPS
2 Distinguish server authentication and client authentication.

Description

Any arbitrary client can initiate communication with a server by sending messages to an IP/port combination. It is up to the server to respond or not. Using server authentication (website running over HTTPS) the client is assured of the server's identity. But in this exercise, the secure server will sustain communication with a known (previously authenticated) client only. This is client authentication.

Steps

Install a Website

1 Go to Internet Information Services (IIS) Manager.
2 Double-click the server name so that you see all of the Web sites. In IIS 6.0, expand Web Sites
3 Right-click the Web Sites and select **new -> website**.(website 2)
4 Fill in a name and click **Next**
5 Fill in the computer's IP and a port and click **Next**
6 Fill in a path and click **next.** (We used C:\Inetpub\wwwroot\test).
7 Similarly create a website 1 in SBS2003.

Questions

1 Can you open the website1 using a browser in WinSrv2003? (……………………………)
2 Can you open the website2 using a browser in SBS2003? (……………………………)

Transforming the HTTP website to use server authentication using HTTPS

1 Go to Internet Information Services (IIS) Manager.
2 Double-click the server name so that you see all of the Web sites. In IIS 6.0, expand Web Sites
3 Right-click the Web site on which you want to install the certificate, and then click Properties. Should be the website you just created.
4 Click the Directory Security tab, and then click Server Certificate under Secure Communications to start the Web Server Certificate Wizard. Click **Next**.

5 Select Create a new certificate and click **Next**.
6 Select Prepare the request now, but send it later and click **Next**.
7 Type a name for the certificate. Select a bit length of 1024; the higher the bit length, the stronger the certificate encryption.
8 Type your organization name and the organizational unit (for example, test and Demonstration). Click **Next**.
9 Type either the fully qualified domain name (FQDN) or the server name as the common name. Click **Next**.
10 Enter your location information, and then click **Next**.
11 Type the path and file name to save the certificate information to, and click **Next** to continue.
12 Verify the information that you have typed, and then click **Next** to complete the process and create the certificate request.
13 Load the certificate request into certification authority
14 Issue pending certificate and export it out to a file
15 Go back to directory security tab and click Server Certificate.
16 Click Process Pending Certificate Request and Install the Certificate
17 Select the newly issued server certificate
18 Enter a port number and click N**ext** till finish**.**
19 On the Directory Security tab, under Secure Communications, note that there are now three available options. To set the Web site to require secure connections, click Edit. The Secure Communications dialog box appears.
20 Select Require Secure Channel (SSL), require client certificates, and then click **OK**.

Questions

1 Using a browser in SBS2003, can you connect to Webserver2 to the secure connection? (…………………..……..)

2 If no, please mention why it was not working and how you solved the problem?
(…………………………………………………………………………..)
(…………………………………………………………………………..)
(…………………………………………………………………………..)

Transforming a secure website using HTTPS to require client authentication

1 Go to Internet Information Services (IIS) Manager.
2 Double-click the server name so that you see all of the Web sites. In IIS 6.0, expand Web Sites
3 Right-click the Web site for which you want to enable SSL and click Properties.
4 On the Directory Security tab, under Secure Communications, note that there are now three available options. To set the Web site to require secure connections, click Edit. The Secure Communications dialog box appears.
5 Select Require Secure Channel (SSL), require client certificates, and then click **OK**.
6 Click **Apply** and then **OK** to close the property sheet.
7 Browse to the site and verify that it works. To do this, follow these steps:

a. Access the site through HTTP in the browser. You receive an error message that resembles the following: HTTP 403.4 **-** Forbidden: SSL required.

b. Try to browse to the same Web page using a secured connection (HTTPS) in the browser. You may receive a security alert that states that the certificate is not from a trusted root

CA. Click Yes and use your certificate to continue to the Web page. If the page appears, you have successfully installed your certificate.

Questions:

1 Whats the significance of server certificate, client certificate to trust?
(…………………………………………………………………………..……………..)
(…………………………………………………………………………..………………..)
2 Does client 2 have access to client authenticated website 1? (…………….)
3 Does client 2 have access to client authenticated website 2? (…………….)

Exercise 4: Certificate Revocation List (CRL)

Objective

Demonstrate the use of CRLs for subordinate CAs as well as for users.

Description

Certificates are used to denote trust relationships. When the certificate issuer no longer trusts the certificate holder, the certificate is revoked. This revoked certificate is published as a list, which is then downloaded and installed by the clients (in this case IE7 or Firefox browsers).

Steps

Revoking PKI user certificates

1 In the SBS2003, open the certificate manager and locate the certificate for client 1.
2 Revoke the certificate issued to the client 1 by right-clicking and following the process.
3 Make sure that the focus (cursor highlight) is on Revoked certificates
4 From menu | Tools | Tasks | Publish CRL and choose all revoked certificates.
5 Then export the CRL to WinSrv2003 and install it in either the IE7 or Firefox browser. For installing on IE7, just right click on the CRL and install. For Firefox, go to menu | Tools | Options | Advanced | Revocation List and enter `\\<IP_of_SBS2003>`. And accept all changes.
6 Can client 1 connect to the client authenticated website 2? (………………………………..)

Revoking PKI user certificates

1 In the SBS2003, open the certificate manager and locate the certificate for subordinate CA.
2 Revoke the certificate issued to the subordinate CA by right-clicking and following the process.
3 Make sure that the focus (cursor highlight) is on Revoked certificates
4 From menu | Tools | Tasks | Publish CRL and choose all revoked certificates.
5 Then export the CRL to WinSrv2003 and install it in either the IE7 or Firefox browser. For installing on IE7, just right click on the CRL and install. For Firefox, go to menu | Tools | Options | Advanced | Revocation List and enter `\\<IP_of_SBS2003>`. And accept all changes.
6 Can client 2 connect to the client authenticated website 2? (………………………………..)

Questions

1 Why could client 2 connect to website 2? Or why not? Explain briefly.
(…………………………………………………………………………..……………..)

Part IV: Appendix A :: Roll back PC to original state.

1 Revoke all certificates created
2 Delete all personal certificates, intermediate CA, root CA from browser as well as CRLs..
3 Remove certificate authority from windows 2003 server. But do not remove SMB CA.
4 Remove certificates from the secure websites.

References

- http://www.csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf
- http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/advcert.mspx
- http://technet2.microsoft.com/windowsserver/en/library/b1ee9920-d7ef-4ce5-b63c-3661c72e0f0b1033.mspx