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