PRINCIPLES OF SYSTEM SECURITY

IS 336: ASSIGNMENT 2

REGNO.: 2017-04-07311

NAME: WESTON, BARAKA

Qn1. Study and explain how the SSL protocol functions. Give the security improvements made from SSL1 to SSL3 (2pages)

SSL stands for Secure Socket Layer and it refers to a protocol for securing communication on the internet. The SSL record protocol provides basic security services to various higher layer protocols, the three higher-layer protocols are defined as part of SSL; the handshake protocol, the change cipher spec protocol, and the alert protocol.

The SSL Record Protocol provides two services for SSL connections:

Confidentiality: The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads.SSL works through the use of public key
Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

Consider the following SSL Record Protocol the working of each;

Change Cipher Spec Protocol; The Change Cipher Spec Protocol is the simplest protocol which consists of a single message with a single byte with the value 1.The purpose of this message is to cause the pending state to be copied into the current state, which updates the cipher suite to be used on this connection.

Alert Protocol; The Alert Protocol is used to convey SSL-related alerts to the peer entity. As with other applications that use SSL, alert messages are compressed and encrypted, as specified by the current state. Each message in this protocol consists of two bytes. The first byte takes the value warning (1) or fatal (2) to convey the severity of the message. If the level is fatal, SSL immediately terminates the connection.

Handshake Protocol; This protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data sent in an SSL record. The Handshake Protocol is used before any application data is transmitted. The Handshake Protocol consists of a series of messages exchanged by client and server

SSL works through the use of cryptography. Public key cryptography uses two keys a public key and private key to transmit secure data between two systems.

Step-by-step how SSL works

- **Establish Security Capabilities;**
  This phase is used to initiate a logical connection and to establish the security capabilities that will be associated with it.

- **Server Authentication And Key Exchange;** The server begins this phase by sending its certificate if it needs to be authenticated; the message contains one or a chain of X.509 certificates. The certificate message is required for any agreed-on key exchange method except anonymous Diffie-Hellman. The final message in this step, and one that is always required, is the *server_done message*, which is sent by the server to indicate the end of the server hello and associated messages.
- **Client Authentication And Key Exchange;** Upon receipt of the *server_done message*, the client should verify that the server provided a valid certificate (if required) and check that the *server_hello* parameters are acceptable. If all is satisfactory, the client sends one or more messages back to the server. If the server has requested a certificate, the client begins this phase by sending a certificate message. If no suitable certificate is available, the client sends a *no_certificate alert* instead
- **Finish;** This phase completes the setting up of a secure connection. The client sends a *change_cipher_spec* message and copies the pending CipherSpec into the current CipherSpec. The finished message verifies that the key exchange and authentication processes were successful.

The improvement made from SSL1 to SSL3 are as follows;

SSL1: This version was first developed by Netscape in 1994 but due to some security weaknesses it was never publicly released.

SSL2: This version was first developed in 1995 by Netscape which came as stronger version than SSL1.

SSL3: This version was designed by Netscape and Paul Koulcher with the elimination of security weakness of the previous versions. Some major improvement of SSL3 over SSL2 are:

- Separation of the transport of data from the message layer
- Use of full 128 bits of keying material even when using the Export cipher
- Ability of the client and serve to send chains of certificates, thus allowing organizations to use certificate hierarchy which is more than two certificates deep.
- Implementing generalized key exchange protocol, allowing Diffie-Hellman and Fortezza key exchanges as well as non-RSA certificates.
- Allowing for record compression and decompression
- Ability to fall back to SSL2 when a 2 client is encountered.

Qn2. Study and explain how the TLS protocol functions. Give the security improvements made from TLS1 to TLS3. Outline the cipher suits involved. (2pages)

TLS stands for Transport Layer Security and refers to a cryptographic protocol that provides end-to-end security of data sent between applications over the internet. It is mostly familiar to users through its use in secure web browsing, and in particular the padlock icon that appears in web browsers when a secure session is established.

How the TLS protocol works

TLS can be used on top of a transport layer like TCP. There are three main components of TLS: Encryption, Authentication, and Integrity.

A TLS connection is initiated using a sequence of known as the TLS handshake. The TLS handshake establishes a cipher suite for each communication session. The cipher suite is a set of algorithms that specifies details such as which shared encryption keys, or session keys, will be used for a particular session. TLS is able to set the matching session keys over an unencrypted channel.

The handshake also handles authentication, which usually consists of the serve proving its identity to the client. This is done using public keys. Public keys are encryption keys that use one-way-encryption, meaning that anyone can unscramble data encrypted with the private key to ensure its authenticity, but only the original sender can encrypt data with private key.

Once data is encrypted and authenticated, it is then signed in with a message authentication code (MAC). The recipient can then verify the MAC to ensure the integrity of the data.

The security improvement made from TLS1 to TLS3 are:

Enhanced security

TLS version 2 is secure so long as its's configured correctly, but improper configuration can leave websites open to cyber-attacks. To offer better protection, TLS3 has done away with numerous obsolete features that have known vulnerabilities including;

- 3DES
- AES-CBC
- Arbitrary Diffie-Hellman groups
- Export ciphers
- DES
- RSA key transport
- SHA-1
- MD5

Because the new protocol has been simplified, administrators are less likely to make mistakes that leave websites open to attacks during configuration.

The cipher suites involved in TLS protocol are;

- **Key exchange algorithm**- is used to exchange a key between two devices, this key is used to encrypt and decrypt the messages being sent between two machines to ensure data confidentiality

- **Bulk encryption algorithm –** is used to encrypt the data being sent. AES, 3DES and CAMELLA are some of the most common algorithms in this category
- **Message authentication code (MAC)-**The MAC algorithm provides data integrity checks to ensure that the data sent does not change in transit

Qn3. On 2 pages explain how the the PKI work. Give PKI enhancements/improvemets made to date.

PKI stands for Public key infrastructure which is the framework or encryption and cybersecurity that protects communications between the server and the client. It works by using two different cryptographic keys: a public key and a private key. The public key is available to any user that connects with the website.

PKI works in the following ways:

A public key infrastructure requires several different elements for effective use.

A certificate Authority (CA) is used to authenticate the digital identities of the users which can range from individuals to computer systems to servers. Certificate Authorities prevent falsified entities and manage the life cycle of any given number of digital certificates within the system.

Second is the component of a Registration Authority (RA), which is authorized by the certificate Authority to provide digital certificates to users on a case-by-case basis. All of the certificates that are requested, received, and revoked by both the certificate Authority and the Registration Authority are stored in an encrypted certificate database.

Certificate history and information is also kept on what is called a certificate store, which is usually grounded on a specific computer and acts as a storage space for all memory relevant to the certificate history, including issued certificates and private encryption keys.

By hosting these elements on a secure framework, a public key infrastructure can protect the identities involved as well as the private information used in situations where digital security is necessary, such as smart card logins and more.

PKI improvements to date

- **PKI for Internet of Things (IoT)**
  Manufacturers of IoT devices are becoming educated on the importance of implementing security into their products. Regardless of the simplicity of each individual device, the IoT presents great security risks due to its sheer scale, which is likely to increase by billions of devices in the next few years.The improvement is on to enable PKI for IoT or PKI4IoT.