Computer Security 1

Assignment 4

Q1) Explain briefly why we need to involve a secure one-way hash function in generating digital signatures.

Ans) The use of one-way hash function in the digital signature is it allows us to provide authentication, non-repudiation and integrity to a particular document. A fundamental characteristics of hashing algorithm is that 2 different messages will not have the exact same hash values, that means a single change in the message will produce a different hashing output. The message is then digitally signed and transmitted to the recipient. The recipient then creates their own hash of the message and uses the senders public key to decrypt the sender's hash. Then the receiver checks his hash with the sender's one, if match found then the sender is verified.

Q2) What is the "digital envelop"?

Ans) Digital envelope is the combination of session key and encrypted message. In digital envelope the session key is encrypted with the receiver's public key and attached to the encrypted message. When he receives the message, he first decrypts the session key using his own private key. By using the digital envelope, only the trusted receiver can only decrypt the message.

A digital envelope uses the two-layer encryption one is secret key encryption on another hand public key encryption. In the secret key encryption, original message is encrypted with the secret key encryption. The session key is then encrypted with the public key encryption.

Q3) **In GSM,**

(a) We assume that each subscriber has been assigned an IMSI (i. e. International Mobile Subscriber Identity) and this information is publicly known. If we want to provide a service to hide this information even during the initial connection (i.e. including the registration), suggest one solution to satisfy this requirement. You need to point out how and why this solution can protect IMSI. (no more than 30 words)

Ans) Instead of the IMSI, a randomly generated temporary mobile subscriber identity is sent to ensure that the mobile subscriber's identity remains confidential and eliminates the need to transfer it in an undeciphered fashion over radio links.

3b) Multiple SRESs and RANDs are stored at VLR for authentication purpose, where SRES=A3(Ki, RAND) and Ki is a pre-shared secret key between the mobile subscriber and HLR. SRES needs to be protected and used as evidence to collect service fee. Since SRES is known by both mobile subscriber and VLR, repudiation cannot be resolved. If we want to establish a partially non-repudiation services between the mobile subscriber and VLR, suggest one solution to meet this requirement. (no more than 30 words)

Ans) Only a public-key system using digital signatures can provide true non-repudiation service among HLR, VLR, and MS. In a public-key system, a digital signature can be used to replace HMAC.

Q4) In most wireless communications, there are 3 entities involved in connecting a call: Mobile Subscriber (MS), VLR, and HLR.

(a) Suggest a method that MS can protect its identity when MS roams into a new VLR region. (i.e. MS does not need to expose its real identity to the attacker when makes the first connection through VLR)

Ans) Registration and Distribution of Authentication Information (Initial Authentication):

When a mobile user (MS) leaves his home domain and roams to a previously visited domain, this procedure is used. The user may make a service request to the network operator of the visited domain. In this case, the three parties perform the initial authentication shown in Figure 3. First, the MS generates a request message and sends it to the authentication VLR/SN in the visited domain. Because the VLR/SN is unable to authenticate the MS on its own, it forwards it to the HLR in the MS's home domain. The HLR is in charge of the verification procedure. The authentication vector is used to generate a response message corresponding to the authentication result (AV). According to the authentication result, the VLR/SN forwards the response message to the MS and decides whether or not to provide the service to the MS. The VLR/SN caches some authentication information in this location, which can be used in subsequent authentication. The response message informs the MS whether or not the authentication was successful. Following the initial authentication, both the VLR/SN and MS obtain the authentication result from the HLR/HN and share some confidential information without the intervention of the HLR/HN.

Q4b) If only VLR and HLR have digital certificates, can a secure channel be established between the MS and VLR? (If your answer is YES, you need to explain how.)

Ans) Authentication and Key Agreement (Subsequent Authentication): Following initial authentication, the VLR/SGSN can authenticate the MS in subsequent communication. If the MS remains in the same visited domain and requests services, the user should request additional authentication. Similarly, the MS generates an authentication request message, which should include the information shared by the MS and VLR/SN; the VLR/SN then uses this information to authenticate the MS. As previously stated, the VLR/SN has cached the information required to authenticate MS. After authenticating the MS, the VLR/SSN sends the MS a response message containing the authentication result. The MS receives the response message and determines whether or not the authentication was successful.

Q5) In SSL and TLS, why is there a separate Change Cipher Spec Protocol rather than including a change_cipher_spec message in the Handshake Protocol?

Ans) SSL uses some messages that are encoded upon the records. On per the record basis the encryption will be done. However, the same type message can be grouped together in the same type records. The encryption settings are modified by the change in cipher spec, a new record should start afterwards so that the settings are newly and immediately updated and is applied. It is very important that the finished messages use Mac and new encryption.

The way to enforce the property is by using a particular record type to change the cipher spec in a way. The SSL/TLS begins in new record for the completed finished message as it uses a record

type distinct from the type of the change cipher spec message. That type can be ignored or avoided if all the SSL/TLS implementations were make enough to start a new record whenever they are required and they need to verify that the peer also began a new one it will be safer and more robust.

Q6) What steps are involved in the SSL Record Protocol transmission?

Ans) The various steps involved in the SSL record protocol transmission are, first it takes the application message and went through with the steps like fragmentation, optional compression, applies MAC, encrypts and then add header to it. Let's take a look into each step briefly.

Fragmentation: Each upper layer message is fragmented into 2 ^ 14, which is 16384 bytes or less blocks.

Compression: This is used optionally and must be lossless. You cannot increase the length of the content by more than 1024 bytes.

Calculate a MAC (Message Authentication Code): A shared secret key must be used for this.

The calculation is defined as following:

hash (MAC_write_secret || pad_2 || hash (MAC_write_secret || pad_1 || seq_num ||

SSLCompressed.type || SSLCompressed.length || SSLCopressed.fragment))

|| = concatenation

MAC_write_secret = shared secret key

hash = cryptographic hash algorithm, either MD5 or SHA-1

pad_1 = the byte 0x36 (0011 1100) repeated

48 times for MD5 & 40 times for SHA-1.

pad_2 = the byte 0x5C (0101 1100) repeated 48

times for MD5 and 40 times for SHA-1

seq_num = the sequence for this message

SSLCompress.type = the higher-level protocol used to process this fragment.

SSLCompressed.length = the length of the compressed Fragment.

SSLCompress.fragment = the compressed fragment

Encryption: Including MAC, the compressed message is encrypted with symmetrical encryption and must not be longer than 1024 bytes.

The next step is to append generated MAC to compressed data and send the whole block for symmetric encryption. This encryption should not raise the length of this block to greater than 1024 bytes. Some of the allowed encryption algorithms are AES, RC2-40, ES, Fortezza, etc. These algorithms are used on the application where SSL used, like somewhere stream encryption is required while at other places Block cipher is required.

Prepare a header in the following fields:

Content Type (8 bits): - The compression method used to compress the enclosed fragment data.

Major Version (8 bits): - The major version of SSL used right now.

Minor Version (8 bits): - The minor version of SSL used right now.

Compressed Length (16 bits): - The length in bytes of the uncompressed data stored in the fragment.