ASSIGNMENT – 4

COMPUTER SECURITY

1)

A hash function turns any piece of digital information, let's imagine, a string as an instance, into a fixed-length string. This is seemingly random. That give-up result is known as a hash. Why is it useful?

The residences are given a collision-resistant cryptographic hash characteristic:

The same input information yields the identical hash whenever. Locating the input data (the preimage) given the hash is challenging with a classical computer. It won't produce the proper result (a collision, however, the original preimage). It is complicated to discover two strings with the same hash. A moderate change in entering data completely adjustments the hash called the avalanche effect. This means that hash is difficult to expect. This indicates that hashes can be used to construct a cryptographic pseudo-random number generator (CSPRNG), password verification without storing a password, and short identifiers for statistics. I can also use them to generate proofs, including a Merkle tree. Digital signature schemes from time to time appoint CRHFs to signal and confirm signatures. Given a few input facts, hash it, and encrypt the hash with a private key (referred to as signing). The cease result is known as a signature, and it can be demonstrated with the aid of decrypting the signature with the public key and hashing the input information to peer if the two suit. It's far challenging to signal something without the personal key.

2)

A digital envelope is a secure electronic data container used to protect a message through encryption and data authentication. A digital envelope allows users to encrypt data with the speed of secret key encryption and the convenience and security of public-key encryption. The Public-Key Cryptography Standard (PKCS) #7 by Rivest, Shamir, and Adleman (RSA) specifies the use of cryptography to data for digital envelopes and digital signatures. Digital envelopes, sometimes known as digital wrappers, are a type of digital envelope. A digital envelope has two layers of encryption: secret (also known as symmetric key) and public (also known as public key). Secret key encryption is mostly used for encoding and decoding messages, whereas public key encryption is primarily used to deliver a secret key across a network to a receiving party. This method does not necessitate the use of plain text communication. The two approaches for creating a digital envelope are as follows:

i)Secret key encryption methods are used to encrypt messages.

ii)RSA's public key encryption algorithm. This is used to encrypt secret keys using a receiver's public key

3a)

Instead of the IMSI, a randomly generated temporary mobile subscriber identification is supplied to ensure that the mobile subscriber's identity stays private and avoids the need to transfer it via radio links in an undeciphered form.

3b)

Only a public-key system using digital signatures can provide accurate non-repudiation service among HLR, VLR, and MS. A public-key system can use a digital signature to replace HMAC.

4a)

Registration and Distribution of Authentication Information (Initial Authentication): When a mobile user (MS) leaves his home domain and roams to a previously visited part, this procedure is used. The user may make a service request to the network operator of the visited component. In this case, the three parties perform the initial authentication. First, the MS generates a request message and sends it to the authentication VLR/SN in the visited domain. Because the VLR/SN cannot 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 generates 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 to provide the service to the MS. The VLR/SN caches some authentication information in this location, 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.

4b)

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, including 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 establish MS. After establishing the MS, the VLR/SSN sends the MS a response message containing the authentication result. The MS receives the response message and determines the authentication was successful or not.

5)

Using a specific record type for Change Cipher Spec is a way to enforce this property. An SSL/TLS implementation cannot help but begin a new record for the finished message since it uses a record type distinct from the Change Cipher Spec message. Such a specific record type could be avoided if all SSL/TLS implementations were disciplined enough to begin a new record where they needed and verify that the peer also started a new record. It is safer and more robust to make it unavoidable through the record type. SSL and TLS were developed or, you may say, designed for the security of transactions for HTTPS. In SSL and TLS, there is a separate change Cipher Spec Protocol rather than including a change cipher spec message in the Handshake Protocol because different cipher Spec protocol is required for signal transitions in ciphering strategies which can send without any Handshake Protocol.

6)

1. Fragmentation: Each upper-layer message is fragmented into blocks of 2^14 bytes or less.

2. Compression: Compression is applied, and it must be lossless and may not increase the content length by more than 1024 bytes. The default algorithm is null in SSLv3 because no compression algorithm is specified.

3. Message Authentication Code (MAC): A MAC must be computed. A shared secret key is used here.

4. Encryption: The compressed message (including the MAC) is encrypted using symmetric encryption. The encryption must not increase the length by more than 1024 bytes, so the total length may not exceed 2^14 + 2048.

5. The final step is to prepare a heading in the following fields: Content Type (8 bits); Major Version (8 bits); Minor Version (8 bits); Compression Length (16 bits)