Chapter 14

1) What are X.509 certificates? What values are stored in an x.509 certificate?

X.509 defines a framework for the provision of authentication services by theX.500 directory to its users. The directory may serve as a repository of public-key certificates .Each certificate contains the public key of a user and is signed with the private key of a trusted certification authority. In addition, X.509 defines alternative authentication protocols based on the use of
public-key certificates.

Created by a trusted Certification Authority (C A) and have the following elements:

Version
Serial number
Signature algorithm identifier
Issuer name
Period of validity
Subject name
Subject's public-key information
Issuer unique identifier
Subject unique identifier
Extensions
Signature

2) What attacks are prevented with certificates?

Certificate Authorities, define an SSL Certificate as a security measure that protects your website from man-in-the-middle attacks. It ensures that your customers' connection, their data, your website and your company are all secure. Let's find out how an SSL Certificate protects you from the cyber attacks known as "man-in-the middle attacks.

Authentication certificates : Secure/Multipurpose Internet Mail Extensions, S/MIME lets you digitally sign your email with a Digital Certificate unique to every person. This ties your virtual identity to your email and gives your recipients the assurance that the email they received actually came from you (as opposed to a hacker who access your mail server).

SSL/TLS Certificates: If your website still uses the more vulnerable HTTP protocol, it's time to upgrade to the safer HTTPS protocol through SSL/TLS Certificates. A TLS Certificate will activate the HTTPS protocol, which is the safer version of HTTP. This allows an encrypted, secure connection between your server and your clients' computers, keeping all information from prying hackers.

3) How do users in the internet use certificates to authenticate servers?

Certificate-Based Authentications actually work. When presented with a certificate, an authentication server will do the following (at a minimum):

1. Has the Digital Certificate been issued/signed by a Trusted CA?
2. Is the Certificate Expired – checks both the start and end dates
3. Has the Certificate been revoked? (Could be OCSP or CRL check)
4. Has the client provided proof of possession?
   https://www.networkworld.com/article/2226498/infrastructure-management-simply-put-how-does-certificate-based-authentication-work.html

4) Who provides trust in a PKI system?

• Initialization: Before a client system can operate securely, it is necessary to install key materials that have the appropriate relationship with keys stored elsewhere in the infrastructure. For example, the client needs to be securely initialized with the public key and other assured information of the trusted CA(s), to be used in validating certificate paths.

• Revocation request: An authorized person advises a CA of an abnormal situation requiring certificate revocation. Reasons for revocation include private-key compromise, change in affiliation, and name change.

Chapter17)

1) Describe the TLS protocol.

Transport Layer Security (TLS) is a protocol that provides a secure channel between two communicating applications. The secure channel has 3 properties:

a. Confidentiality: Nobody other than the two ends of the channel can see the actual content of the data transmitted.

b. Integrity: Channel can detect any changes made to the data during transmission

c. Authentication: At least one end of the channel needs to be authenticated, so the other end knows who it is talking to.

2) Where does the TLS protocol sit in the Internet layers?

- TLS sits between the Transport and Application layer
  – Unprotected data is given to TLS by Application layer
  – TLS handles encryption, decryption and integrity checks
  – TLS gives protected data to Transport layer

3) What attacks are prevented with the TLS protocol?

Renegotiation Attack
Rc4 attacks
Change cipher spec injection attack
Poodle attack
Protocol downgrade

4) What is the purpose of using a nonce in the TLS protocol?

In SSL/TLS handshake, a nonce is always sent by the client to server and vice versa. The nonce basically consists of a random number and unix timestamp. Why do we need the unix timestamp?

As the nonce is always a random number, how does this protect from replay attack by a man-in-the-middle? Being a random thing, same nonce might be repeated in another handshake with the same server.

5) Can an internet router eavesdrop on TLS traffic? No

6) HTTP vs HTTPS

1. HTTP URL in your browser's address bar is http:// and the HTTPS URL is https://.
2. HTTP is unsecured while HTTPS is secured.
3. HTTP sends data over port 80 while HTTPS uses port 443.
4. HTTP operates at application layer, while HTTPS operates at transport layer.
5. No SSL certificates are required for HTTP, with HTTPS it is required that you have an SSL certificate and it is signed by a CA.
6. HTTP doesn't require domain validation, where as HTTPS requires at least domain validation and certain certificates even require legal document validation.
7. No encryption in HTTP, with HTTPS the data is encrypted before sending.

Homework problems

17.3 Consider the following threats to Web security and describe how each is countered by a particular feature of TLS.

a. Brute-Force Cryptanalytic Attack: An exhaustive search of the key space for a conventional encryption algorithm.
b. Known Plaintext Dictionary Attack: Many messages will contain predictable plaintext, such as the HTTP GET command. An attacker constructs a dictionary containing every possible encryption of the known-plaintext message. When an encrypted message is intercepted, the attacker takes the portion containing the encrypted known plaintext and looks up the ciphertext in the dictionary. The ciphertext should match against an entry that was encrypted with the same secret key. If there are several matches, each of these can be tried against the full ciphertext to determine the right one. This attack is especially effective against small key sizes (e.g., 40-bit keys).
c. Replay Attack: Earlier TLS handshake messages are replayed.
d. Man-in-the-Middle Attack: An attacker interposes during key exchange, acting as the client to the server and as the server to the client.
e. Password Sniffing: Passwords in HTTP or other application traffic are eavesdropped.
f. IP Spoofing: Uses forged IP addresses to fool a host into accepting bogus data.
g. IP Hijacking: An active, authenticated connection between two hosts is disrupted and the attacker takes the place of one of the hosts.
h. SYN Flooding: An attacker sends TCP SYN messages to request a connection but does not respond to the final message to establish the connection fully. The attacked TCP module typically leaves the "half-open connection" around for a few minutes. Repeated SYN messages can clog the TCP module.

17.4 Based on what you have learned in this chapter, is it possible in TLS for the receiver to reorder TLS record blocks that arrive out of order? If so, explain how it can be done. If not, why not?

17.3

a. Brute Force Cryptanalytic Attack: The conventional encryption algorithms use key lengths ranging from 40 to 168 bits.

b. Known Plaintext Dictionary Attack: TLS protects against this attack by not really using a 40-bit key, but an effective key of 128 bits. The rest of the key is constructed from data that is disclosed in the Hello messages. As a result the dictionary must be long enough to accommodate 2128 entries.

c. Replay Attack: This is prevented by the use of nonces.

d. Man-in-the-Middle Attack: This is prevented by the use of publickey certificates to authenticate the correspondents.
e. Password Sniffing: User data is encrypted.
f. IP Spoofing: The spoofer must be in possession of the secret key as well as the forged IP address.
g. IP Hijacking: Again, encryption protects against this attack.
h. SYN Flooding: TLS provides no protection against this attack.
17.4 TLS relies on an underlying reliable protocol to assure that bytes are not lost or inserted. There was some discussion of reengineering the future TLS protocol to work over datagram protocols such as UDP, however, most people at a recent TLS meeting felt that this was inappropriate layering.

3 Chapter 20- IPsec

1) Where does the IPsec protocol sit in terms of the Internet layers?

Network Layer (layer 3)
IPSec is a suite of protocols that provide security services at IP layer of TCP/IP stack i.e. Network Layer in OSI model. AH provides authentication, integrity and anti-replay services at Network Layer and above.

2) Describe the IPsec protocol.

In computing, Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs).
IPsec includes protocols for establishing mutual authentication between agents at the beginning of a session and negotiation of cryptographic keys to use during the session. IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).[1] IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. It supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection.
The initial IPv4 suite was developed with few security provisions. As a part of the IPv4 enhancement, IPsec is a layer 3 OSI model or internet layer end-to-end security scheme, while some other Internet security systems in widespread use operate above layer 3, such as Transport Layer Security (TLS) and Secure Shell (SSH), both of which operate at the Application layer. IPsec can automatically secure applications at the IP layer.

3) Can a TLS connection run over an IPsec tunnel?

TLS/SSL is not a single application like SSH, but provide security through implementation into applications. SSL was designed by Netscape2 with HTTP usage in mind. TLS is the latest

version of the SSL technology. IPsec provides security at the IP packet layer; it is not integrated at higher levels like TLS/SSL.

4) In what cases would it be preferable to run IPsec instead of TLS?

TLS is a protocol working over TCP and you already use it in many applications, like HTTPS, SMTPS, NNTP (port 563), FTPS, etc. The main use is related to HTTP, for web browsing (especially for e-commerce). In these cases, often only the server is authenticated.

You cannot use TLS, for instance, in many real-time applications, since they are not based on TCP, but on UDP.

IPsec is a level 3 protection method could be used, for example, for establishing a VPN connection, maybe among multiple company offices. Since TCP/UDP packets are encapsulated in IP datagrams, you can use IPsec to hide some level 4 informations like session numbers or source/destination ports. IPsec can hide also the IP datagram's header itself, so you can avoid the attacker to do traffic analysis. Both things that with TLS you cannot do.

You cannot use IPsec with NAT, because the latter modifies values in the headers which interfere with the integrity checks done by IPsec.

. Can an Internet router eavesdrop IPsec traffic? No

. Can a device inside the LAN eavesdrop on IPsec traffic?