Md. Safiqul Islam
islam3@kth.se

IK2206 Internet Security and Privacy, 2007
Assignment 3: PKI, IPsec, SSL/TLS

1. The IPsec specification defines two modes of applying IPsec protection to a packet.
a) What are the two modes?

Answer: Transport mode and Tunnel mode.

b) What is the difference between the two modes when it comes to providing protection?

Answer: Transport mode provide end to end security whereas tunnel mode provide gateway to gateway security or gateway to end security.

c) Sketch what an IP packet looks like after IPsec protection in the two different modes. You only need to show payload and the different headers (not the individual header fields).

Answer:

Tunnel mode:

AH:

New IP Header | AH | Orig IP header | TCP Header | Data

ESP:

New IP Header | ESP | Orig IP Header | TCP Seg | ESP Trailer |

Transport mode:

AH:

IP Header | AH | TCP Header | Data

ESP:

IP Header | ESP Header | TCP Segment | Data | ESP Trailer | ESP

2. An IPsec security association (SA) is a cryptographically protected connection.
a) What parameters are used to uniquely identify an SA?

Answer: {SPI, Destination, Flag}

b) Name two different methods to set up an SA between to IPsec end-points.
Answer: Main mode and Aggressive mode.

c) Give four examples of information (parameters) included in the SA.

Answer: Cryptographic key, Identity of other end. Sequence number and Cryptographic service.

3. The IPsec specifications define two types of IPsec headers: AH (Authentication Header) and ESP (Encapsulating Security Payload).
a) What is the difference between integrity protection in AH compared to integrity protection in ESP?

Answer: ESP provide integrity protection beyond the IP header (TCP segment). But AH provide integrity on some fields of IP header (Immutable field) and TCP segments.

b) Why can't AH all fields of an IP header be included in the AH's end-to-end integrity check?
Answer: Because some fields have to be checked by the router and firewall during the transmission (TTL field).

c) Why does the ESP header include a padding field?
Answer: To disguise the size of the data and make the data to be a multiple of block size for cryptographic algorithm.

4. IKE (Internet Key Exchange) is a protocol for doing mutual authentication and establishing a shared secret key to create an IPsec SA.
a) What is the purpose with the Diffie-Hellman exchange in IKE phase 1?

Answer: It does mutual authentication and establishes session key.

b) Why does IKE use cookies and nonces?

Answer: Cookies helps us to prevet from DoS attack and Nonces help us from prevent replay attack.

c) Why are there two phases in IKE?

Answer: So that we can reuse the session key established in phase 1 for phase 2 for the session between Alice and Bob. Because mutual authentication in phase 1 is expensive.

5. PKI trust models can be organized in many different ways, such as Monopoly Model, Oligarchy Model, etc.
a) Is it possible to determine, by examining a certificate, what trust model is used within the PKI?

Answer: It will not be possible always because for both the Oligarchy and Anararchy model certificates can be chain of certificate or one single certificate in the chain.

b) Compare the Monopoly Model plus RA to the Monopoly Model with Delegated CAs. In Monopoly Model plus RA, the signing of certificates is done by the CA. Does this make the model more secure? What are the advantages and disadvantages of the two models?
Answer:
For the Monopoly model plus RA , if an one RA is compromised then it can take forged signature from the CA because CA trust RA and rubberstamps the value. Then the entire world will be under security risk.

But for Monopoly model with delegated CA, if any of the CA is compromised then only that CA will be affected but the security of the world is still under risk.

c) Revocation of public key certificates is an important part of PKI. But certificates also carry expiration dates, so there are two ways in which a certificate can be invalidated (revocation and expiration). What are the reasons for having two ways of invalidating certificates? Would it not be sufficient with revocation?

Answer: If we use only revocation then the CRL list will be unmanageable. So adding expiration date to invalidated certificates is to keep the CRL list manageable. So the revoked certificate with expired time can be removed from the list.

6. SSL/TLS is used for secure web communication. It distinguishes between connections and sessions.
a) What is the relationship between a connection and a session? Explain how the handshake protocol is related to sessions and connections?

Answer: Session is relatively long lived thing from which many connections can be established. When two communication parties want to communicate they can establish a session and within the session they can establish several connections between themselves. In the handshake protocol if client and server remember the session_id then next time they can establish connection without computationally intension public key cryptographic computation. They can set up connection from the master secret and nonce sent by them.

b) How does SSL/TLS protect against replay attacks?

Answer: In the handshake protocol of SSL/TLS both client and server uses random numbers (R_A, R_B) which are used to calculate the master secret k. So there here no threat of replay attack exists.

c) HTTP is designed for stateless communication, and a web server does not, in theory, need to keep track of its clients and what they have been doing in the past. Still, most web sites support per-user customization and "stateful" interaction, such as shopping carts. Explain how this is achieved, and some of the different methods that are used to achieve this?

Answer: We can do it by using "cookie" and "session". Cookie is a small information file kept at the client side and is used to track client activities. This is how shopping card information can be retrieved even if client disconnects from the server and connects again. Session is somewhat more restrictive than cookies, it is used to keep history of client while client is browsing through the sites and in this way there is no need to keep anything in client side.