HW-Module9 Results for BRANDEN BARNES

Score for this attempt: 100 out of 100
Submitted Mar 17 at 9:01pm
This attempt took 234 minutes.

Question 1
15 / 15 pts

What purpose does the MAC serve during the change cipher spec SSL exchange?

Your Answer:

The Message Authentication Code (MAC) allows for the authenticity and integrity of a message by generating a unique code used in the Handshake Protocol that helps define a shared key. The purpose it serves during the change cipher spec SSL exchange involves the protection of the integrity of the first round of messaging where cookies will be exchanged. This helps to prevent man-in-the-middle attacks by not allowing for suppression of the original message. The MAC in SSL allows for a fixed-length message.

Question 2
70 / 70 pts

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

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 SSL 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.

Your Answer:

a. SSL uses symmetric one-time session keys. If a hacker were to intercept encrypted data, they would not be able to use it without the proper private key that was used in the decryption process. SSL can also implement a stronger cipher for greater protection during the session.

b. SSL protects against Known Plaintext Dictionary Attack by generating more bits to the 40-bit secret key. This adds an 88-bit disclosed key that as a result provides a 128-bit encrypted key making an attack impractical. This helps in the randomizing of the cipher text.

c. SSL uses time stamps on the first 4 bytes of each session. SSL also uses nonce values making it unlikely to predict in advance. This allows client-to-server operations to be known if it has been tampered with.

d. The SSL can block a man-in-the-middle attack by using mutual authentication with certificates, and the digital signature of a trusted entity which provides a certifying authority. SSL client software allows verification of secure travel with the server's name and public key value.

e. SSL blocks Password Sniffing because passwords are encrypted.

f. SSL blocks IP Spoofing because it doesn't use IP addresses in the authentication process with the client and server.

g. During an IP Hijacking, SSL will leave it unsuccessful because even if the attacker can get into the handshake, he cannot know the encryption key. Also, the attacker will be kicked out during a protocol alert because he can not send data with the wrong key. During handshake, if the attacker does not know the password, he will get the message authenticated.

h. SSL cannot block SYN Flooding because the protocol only starts after a successful TCP handshake.

Question 3

15 / 15 pts

For SSH packets, what is the advantage, if any, of not including the MAC in the scope of the packet encryption?

Your Answer:

The advantage of SSH packets not including the MAC in the scope of the packet encryption is to allow the packet to have better flexibility in handling the encryption process using different encryption styles. This can provide better encryption and authentication for performances that will best suit the packet.

Quiz Score: 100 out of 100