ISA562_Assignment_6 Mithilaesh Jayakumar(G01206238)

Chapter 13

Qn 2

1. It is mentioned in the statement that the replication was done using a simple download with no checks for the cryptographic integrity.
2. By using a cryptographic integrity check, we include a timestamp which is the hash of the file from KDC.
3. A person who tries to impersonate does not have any knowledge of Master Key but still he can modify the KDC.
4. As cryptographic integrity is not performed the impersonator can assign a new master key and this is not included in the timestamp.
5. By doing so he can manipulate the database replacing it with new values.

Qn 3

1. The TGS REQ Authenticator is used to verify the session key knowledge without which the credentials field cannot be decrypted by the ticket requester.
2. But the AP REQ authenticator can be used to prove the knowledge of the shared key.
3. By doing so, the further messages become unencrypted providing no means to authenticate.

Qn 5

1. In Cipher-Block Chaining mode every ciphertext block affects two different plain text blocks.
2. The first is through decryption and the second is through XOR operation.
3. In Propagating or Plaintext Cipher-Block Chaining mode every ciphertext block affects their respective plaintext block by applying the XOR operation on its decryption.
4. Because of this every successive plaintext block is affected, as XOR is applied on the result of the XOR operation as well as on the decryption result.
5. Any set of ciphertext blocks will have effects on the successive plaintext blocks in such a way that it is not dependent on the order of the blocks within these sets of ciphertext blocks.
6. The resulting effect is essentially because of the XOR operation of the XOR operation of every ciphertext block and decryptions.

Chapter 17

Qn 1

1. No. Bob's IPsec implementation will not notice that the packet is a duplicate and it will consider the retransmitted TCP as a new one.
2. IPsec is generally used to provide security at the network layer by encrypting TCP.
3. It is a highly secure and expensive packet by packet cryptography method.
4. Only the TCP protocol is responsible for monitoring of the transmitted TCP packets and ignoring duplicate ones.

Qn 6

Advantages of F1:

- Enables adding new IP header.
- Helps to avoid revealing the original one.
- This new IP header can route the packet.
- F1-F2 shared key can be used for encryption.

Disadvantages of F1:

- Encryption makes the routing process complex because of the added steps from the decryption process.