Rashed Abdulla Alyammahi

1.

a) The mentioned situation violates the security goal of Integrity from CIA Triad.

b) The mentioned situation violates the security goal of Confidentiality from CIA Triad.

c) The mentioned situation violates the security goal of Availability from CIA Triad.

2.

a. Only a single private key K, this is using symmetric encryption

b. Because the three using a same key K and share a same network via wireless, Ted can change receiver address to Alice to trick Alice think that the same message was sent to her.

c. It can prevent the attack in part b because Alice can check the nonce, it’s different from Carol, so she can ignore that message.

d. Bob can attach a Cyclic Redundancy Check (CRC) in last message to verify data is correct or not.

3.

a. Sender has a public key to encrypt message, so only sender can generate message to send to receiver that holding private-key.

b. Receiver will use private key to decrypt the message, only receiver has this key, it’s a pair of public key.

c. public key and private key is a pair to encrypt/decrypt message. Only Sender holds public key and only receiver holds private key, so if receiver can decrypt message, it’s sure the message sent from sender.

4.

Kernel protects from malicious applications that can cause corruption system. Kernel is not effective to prevent the attacks like read memory to look up key because applications need to get secret key to calculate for crypto algorithm. So machine modes for purpose to keep keys that store in security from the attacks like that. For instance, ARM architecture supports TrustZone to store/get secret keys and implement some crypto algorithm.

5.

Memory protection is a way to prevents process affecting other processes. processes own and authorize their memory, page fault mechanism provides hard memory protection boundaries. It is impossible for an unprivileged for a process to access a page that has not been explicitly allocated to it.

6.

A memory protection key mechanism divides physical memory into blocks of a particular size, each of which has an associated numerical value called a protection key.

That can protect your memory from peeking up and faking (integrity).

7.

a. Create a hash table for per-subject access control list.

- Look up the list that can be hashed into a table to determine authorize, O(1).

- Just add a subject to control list hashed table, O(1).

- Delete an access subject from hash table, O(1).

- There need to add object to all subjects, that can take O(n), n is subject number.

b. Create a hash table for per-object access control list.

- Look up the list that can be hashed into a table to determine authorize, O(1).

- Just add a subject to control list hashed table, O(1).

- Delete an access subject from hash table, O(1).

- default access rights for an object can be set, O(1).

c.

- Need to look up a row in matrix, O(n), n is subject number.

- New subject needs to be added to matrix, it depends on implementation, add a new row can takes O(n) time complexity but row is a pointer then the minimum time complexity is O(1).

- Need to look up in row to delete access subject, O(n), n is subject number.

- New object need to be added to matrix, it depends on implementation but if it may just require adding a new entry to an existing table then minimum time complexity is O(1).

8.

We can create a sub-object that show object state(active/inactive), the per-subject control will refer to sub-object. If object is deleted, then sub-object state changes to inactive.