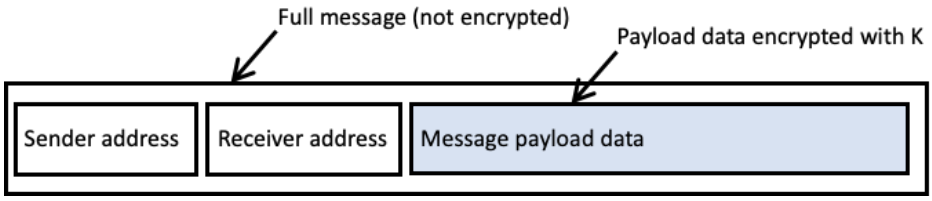
Homework 6
COM S 352
Fall 2021

1. (10 points) Select the security goal from the CIA Triad (confidentiality, integrity and availability) that has been violated in each scenario.

a. A user replaces wininit.exe on a Windows file system with a modified version that contains a backdoor to allow unauthenticated access to the machine in the future.
b. A botnet (a group of compromised Internet-connected devices) is being used to target a webserver with high amounts of network traffic with the objective of overwhelming the server's resources.
c. A user is logged into their account at Secure Bank & Trust, an attacker has launched a man-in-the-middle attack that allows the attacker to observe the communication.

2. (20 points) Suppose three parties Bob, Carol and Alice are part of a wireless network and want to be able to send messages between each other that will be readable by only the three of them. All three share a single private key K. When sending data they constructor a message in format shown below where the message has the sender and receiver addresses in plain text and the data encrypted by K.



a. Is this an example of symmetric or asymmetric encryption?
b. Suppose that Bob sends a message to Carol, how could Ted trick Alice into thinking that the same message was sent to her?
c. A nonce is commonly used to prevent the replay attack, would adding a nonce to the encrypted part of the message (right before the payload data) be sufficient to prevent the attack described in part b?
d. When Bob sends a message to Carol, how will Carol be able to know that the message has not been corrupted? If it is not currently possible, propose a modification to the message format.

3. (15 points) Discuss how the asymmetric encryption algorithm can be used to achieve the following goals.

a. Authentication: the receiver knows that only the sender could have generated the message.
b. Secrecy: only the receiver can decrypt the message.
c. Authentication and secrecy: only the receiver can decrypt the message, and the receiver knows that only the sender could have generated the message.

4. (10 points) Many computer architectures offer more than just two security modes, for example, they have user, kernel and machine mode. If the operating system is trusted to execute with kernel mode privileges, why is there need for a machine mode?

5. (10 points) How do operating systems that use paged virtual memory prevent processes from reading or writing the physical memory of other processes? Be specific about the mechanisms in place that prevent this.

6. (10 points) An operating system provides access control which prevents unauthorized reading of data, what are the advantages of encrypting data stored in the computer system?

7. (15 points) Describe each of the following three kinds of access control mechanisms in terms of (a) ease of determining authorized access during execution, (b) ease of adding access for a new subject, (c) ease of deleting access by a subject, and (d) ease of creating a new object to which all subjects by default have access.

a. per-subject access control list (that is, one list for each subject tells all the objects to which that subject has access)
b. per-object access control list (that is, one list for each object tells all the subjects who have access to that object)
c. access control matrix

8. (10 points) Suppose a per-subject access control list is used. Deleting an object in such a system is inconvenient because all changes must be made to the control lists of all subjects who did have access to the object. Suggest an alternative, less costly means of handling deletion.