**Homework Assignment #2**

**CS 4390 Network Security Scenarios Fall 2021**

**Dr. Rajaei Student Name: Sidney Sanders**

**Due: Dec 1, 2021**

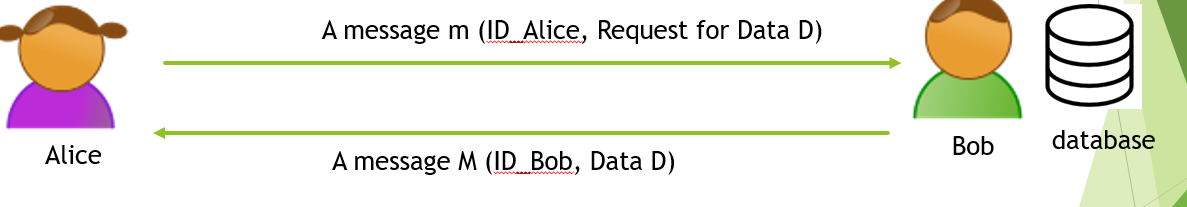
**Total points: 20**

**Reference:** Textbook, Computer Networking, 7th Ed Kurose & Ross; Chapter 8

**Your Task:**

Assume you have Alice and Bob communicating messages via the network. Explain each concept in the following scenarios. Write your answer in a few lines on the give template, add your name, and submit it on Canvas latest on the due date.

* What that scenario means?
* What happens if the sequrity is gone?
* How can we make it secure?



* Confidentiality:

Alice is requesting the data and her request is sent to only bob, Bob then goes and gets the certain data being requested and returns it to Alice and Alice only. In this scenario we want to make sure that the communication between Alice and Bob remains confidential through the entire interaction. To keep this only between Alice and Bob, the information being sent is encrypted to ensure that no one else can intercept the messages between them. Without the security to protect the data being sent, the data could be intercepted or stollen by an outside source.

* Integrity:

This scenario addresses the problem of a potential threat to the validity of the information sent between Alice and Bob. We want to make sure that the messages they receive are what the other had sent. To ensure this, we can use a cryptographic technique that ensures that the message bob received was from Alice, and the message and data Alice receives is truly from Bob. One way could be the hash algorithm to ensure message integrity. Without this added security, false messages could be getting sent by someone other than Alice and Bob.

* Availability:

In this scenario, the availability of Alice and Bob is the public key that people can see to communicate with. Alice needs to have Bobs public key to be able to reach out to him and give him the request for the data. Without the added security to ensure the secure communication between Alice and Bob, there could be false data being sent to Alice, or Bob could be giving data to someone who is not cleared to receive the information. With the public and private keys, Bob and Alice can communicate through Bobs public Key and Bob can use his private key to decrypt the message sent by Alice to receive the message

* Authentication:

This situation resolves the issue of a possible danger to the legitimacy of the data sent among Alice and Bob. We need to ensure that the messages they get are what the other had sent. To guarantee this, we can utilize a cryptographic method that guarantees that the message Bob got was from really from Alice, and the message and information Alice gets is genuinely from Bob. One way could be the hash calculation to guarantee message uprightness. Without this additional security, bogus messages could be getting sent by somebody other than Alice and Bob. This creates a security risk for Bob, we don’t want to release incorrect data to be given to Alice.

* Authorization:

Alice needs a certain level of authorization to reach certain information in the database (Bob). To make sure that she has clearance for information that is requested, Bob will need to check to make sure that Alice is allowed to receive the information she requested. Authorization can be secured using the Public Key Infrastructure (PKI) which will also allow a secure message Integrity. Without this security implemented, Bob and Alice could be communicating with the incorrect users.

* Non-repudiation:

This is contract like situation, when someone agrees to a non-repudiation it protects those in this agreement by saying that who’s ever signature, for example, is signed, that person or device must complete the desired agreement, If Bobs device signature agrees to exchange information, he needs to send Alice the data she requests per their agreement. Without this type of security implemented, Alice could request the correct type of data, but Bob may not send it to her, with this implemented, it guarantees Alice that she will get the information she requires.

* Privacy:

Privacy in this situation, Alice may be communicating with Bob for a one time only reason. In that case, she may not want Bob to remember information about her visit to his server. To obtain some privacy, Alice could use a combination of certain proxy servers, or the use of an SSL. The traffic between Alice and the roxy will ensure the encryption of her information and there for ensure her privacy and will not allow anyone to invade her information. Without this step in the security her information may be logging her visit and may record the data that’s being exchanged between Alice and Bob.