Vivian Do
CSC 4222
Sep 11 2022

CSC4222/6222: Assignment 1

Due at 11:59 pm, Sep. 11

1. 1) Explain the concepts of C.I.A and the tools to achieve C.I.A, respectively. 2) What are the differences between message confidentiality and message integrity? Can you have confidentiality without integrity? Can you have integrity without confidentiality? Justify your answer.

   3) Please Specify and explain which concept(s) each of the following cases violates. **a.** John copies Mary's homework.

   b. Paul crashes Linda's system.

   c. Carol changes the amount of Angelo's check from $100 to $1,000.

   d. Gina forges Roger's signature on a deed.

   e. Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name.

   f. Jonah obtains Peter's credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number. **g.** Henry spoofs Julie's IP address to gain access to her computer.

   h. Jonah sends Peter an e-mail with a 2MB attachment, knowing that Peter's remaining quota for his e-mail account is 2.1MB.

   i. Anna registers the domain name "JohnSmith.com" and refuses to let John Smith buy or use the domain name.

1) CIA stands for Confidentiality, Integrity, and Availability.
   - ❖ Confidentiality is the protection of data by giving access to those who are allowed to see the information without sharing it elsewhere. Two main tools used for confidentiality are encryption and access control.
   - ❖ Integrity is the protection of data against unauthorized alterations of the information. Three tools used for integrity are backups, checksums, and data correcting codes.
   - ❖ Availability is the protection of data of those who are authorized to access the information. Two tools used for availability are physical protections and computational redundancies.

2) Message confidentiality is the original message being sent from sender to receiver cannot be determined by a hacker . Message integrity is the message sent from the sender, whether encrypted or not, can be found altered by the receiver. Yes, you can have one without the other, since these two are two different concepts. An encrypted message can pass as confidentiality, but will not have integrity. The encrypted message can also be detected when sending, but this will not pass as confidentiality.

3a) Confidentiality; the leaked information of Mary's homework is a violation of confidentiality and this was used and stolen by John.

3b) Integrity and Availability; Paul breaking Linda's system is a violation of integrity, and Linda not being able to access her system is another violation of availability.

3c) Confidentiality and Integrity; the amount of Angelo's check is a violation of confidentiality since Carol was able to access this information, and Carol changing the amount in the check is another violation of integrity.

3d) Confidentiality and Integrity; Roger's signature being seen by Gina is a violation of confidentiality, and Gina having access to change his signature is another violation of integrity.

3e) Availability; this is a violation of availability due to Rhonna not willing to let publishing houses acquire that specific domain name.

3f) Confidentiality, Integrity, and Availability; this is a case of all three concepts. Jonah obtaining Peter's credit card information is a violation of confidentiality, Jonah having access to cancel and replace that card is a violation of integrity, and Peter not being able to access his card due to it being linked to a different account number is a violation of availability (because he can't use that card anymore).

3g) Confidentiality; Henry being able to access Julie's computer without her knowing is a violation of confidentiality.

3h) Availability; Jonah knowing that Peter has not enough storage on his email account and still sending him an attachment is a violation of availability.

3i) Availability; similar to Rhonna's case in 3e, this is a violation of availability due to Anna not willing to let John Smith acquire that specific domain name.

2. Compare and contrast symmetric encryption with public-key encryption, including the strengths and weaknesses of each.

Symmetric encryption is when there is a common key used to encrypt and decrypt messages between the sender and the receiver. Some advantages this key has is that it can be extremely secure when using a secure algorithm and it is relatively fast. Some disadvantages this key has is that it involves being shared with another user, and this can cause more damage if this key gets in the wrong hands.

Public-key encryption is an asymmetric form of encryption where messages are being encrypted and decrypted by using two different keys. Some advantages this key has is that it allows for message authentications, it is more convenient since it's public, and it can check for altered messages when received. Some disadvantages this key has is that the process is slower, the public keys are not authenticated since no one knows which public key belongs to whom, and the risks of losing private keys when decrypting messages is higher.

3. What is Authenticity and the tools to achieve Authenticity?
Please Explain: Can Bob violate an agreement with his digital signature or not?

Authenticity is the ability to detect genuine statements, policies, and permissions from systems. One of the tools to achieve authenticity is using digital signatures; this allows a person to have authenticity protection and control over their information in

a unique way.

Yes, Bob is able to violate an agreement with his digital signature. Bob can still risk his digital signature being stolen by an attacker taking his private key. The attacker is then able to modify any documents Bob has signed; this can put Bob in a hazardous situation.

4. Please describe the concept of the following methods of Threats & Attacks and give a protecting method.
   a. Alteration
   b. Denial-of-Services
   c. Correlation and Traceback

a) Alteration is the unauthorized modification of information. A way to protect one's data from an alteration attack is to add an integrity service to prevent the information in the data to not be modified or deleted by any attackers.
b) Denial-of-Services is the interruption or degradation of a data service or information access. A way to protect one's data from a DoS attack is to have a defense mechanism to provide a guard against attackers; this will protect one's availability to their information.
c) Correlation and Traceback is the integration of multiple data sources. Information flows to determine the source of a particular data stream or piece of information. A way to protect one's data from a correlation and traceback attack is to add an a service that detects incoming attack; this can identify the source of the attack and provide ways to block the attacker from leaking any information.

5. Please explain what if a newly designed system without the following Security Principles:
   a. Fail-Safe Default
   b. Complete Mediation
   c. Separation of Privilege

a) Fail-Safe Default: the default configuration of a system should have a conservative protection scheme. The new system will always go to a safe status in the event of any problems approaching.
b) Complete Mediation: every access to a resource must be checked for compliance with a protection scheme. The new system should be able to run a check on the user trying to access the system to see if they are allowed to have access to said object.
c) Separation of Privilege: multiple conditions should be required to achieve access to restricted resources or have a program to perform such action. The new system should divide its program into specific parts to perform its tasks; this is to lessen the damage of the computer security vulnerability when running into a problem.

6. **a.** Can you "decrypt" a hash of a message to get the original message? Explain your answer.
   b. In what way does the public-key encrypted message hash provide a better digital signature than the public-key encrypted message?

a) No, you cannot decrypt a message hash to get the original message. Hash is a

one-way function Y=H(M) but is hard to find M when only given Y. The original message cannot be recovered with any given hash value.

b) A public-key encrypted message hash only needs a private key to encrypt short messages. The hash allows you to encrypt smaller amounts of data in comparison to encrypting a larger message through the regular public-key encrypted message.

7. Bob thinks that generating and storing a random salt value for each userid is a waste. Instead, he is proposing that his system administrators use a cryptographic hash of the userid as its salt. Describe whether this choice impacts the security of salted passwords and include an analysis of the respective search space sizes.

Bob's idea of using a cryptographic hash of *userid* as its *salt* would negatively impact the security of salted passwords.

For every password stored in the system, there is a randomly generated salt value attached to it. This can be processed with a hash function to store the salt in the system. If the salt isn't random, when using it the attacker is able to generate dictionary files for every salt value in the system. This allows them to reduce the salt space when creating dictionaries for the most common *userid*s, giving them an easier way to attack the users.

With a unique salt, the attacker is unable to tell if any two users have the same *userid*, password, and salt value. The attacker cannot determine the same *userid* and password combination are used in more than one system.

8. Suppose you could use all 128 characters in the ASCII character set in a password. What is the number of 8-character passwords that could be constructed from such a character set? How long, on average, would it take an attacker to guess such a password if he could test a password every nanosecond?

The total number of 8-character passwords that can me made from all 128 ASCII characters is 128^8 or $7.2057594038 * 10^{16}$; there are 128 characters that are potentially chosen for every 8-character password.

As for testing every password at every nanosecond (10^{-9}), the attacker would take $128^8 * 10^{-9}$ or 72057594.0379 seconds on average as the worst case scenario.

9. **a.** Barack often sends funny jokes to Hillary. He does not care about confidentiality of these messages but wants to get credit for the jokes and prevent Bill from claiming authorship of or modifying them. How can this be achieved using public-key cryptography?

b. As public-key cryptography is computationally intensive and drains the battery of Barack's device, he comes up with an alternative approach. First, he shares a secret key k with Hillary but not with Bill. Next, together with a joke x, he sends over the value d = h(k||x), where h is a cryptographic hash function. Does value d provide assurance to Hillary that Barack is the author of x and that x was not modified by Bill? Justify your answer.

a) By using public-key cryptography, Barack should digitally sign his jokes with a private key and send each joke together with his signature since he just wants credit for his jokes. Everyone that has received Barack's jokes can use his public key to verify that he signed it.

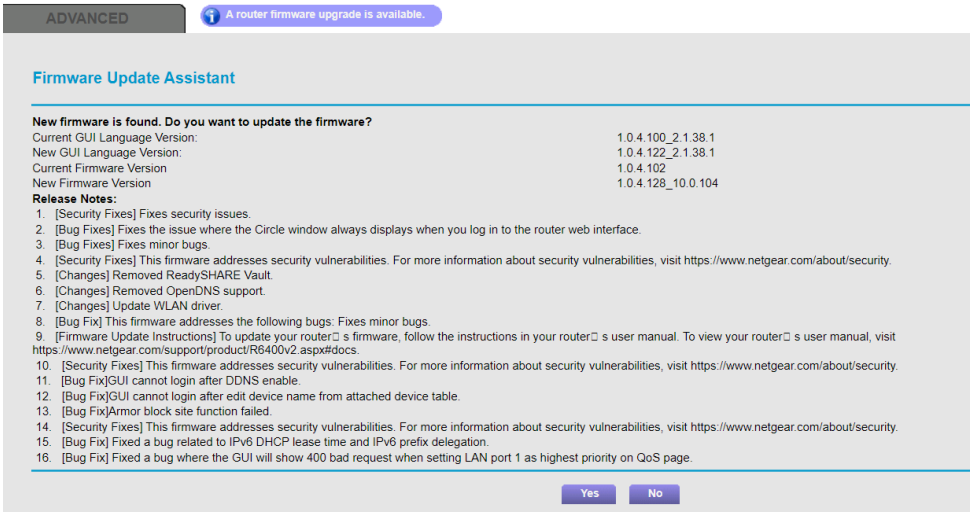
b) Yes, value *d* should provide assurance to Hillary. Since Barack has given her the secret key *k*, Hillary is then able to compute value *d* with *h(k||x)* where *h* is the hash function. This verifies to Hillary that the joke was sent by *x* (Barack). If Bill were to intercept *x* he would not be able to compute *h(k||x)* since Barack's secret key was not shared with him.

10. Check the router (or access point) at your home. List 5 security features your router is using to protect your home network. For each feature, a screenshot and a brief description of its functionality are required.

My family currently uses the NETGEAR AC1750 Smart WiFi Router Model R6400. Below are some of the security features NETGEAR offers through its website:

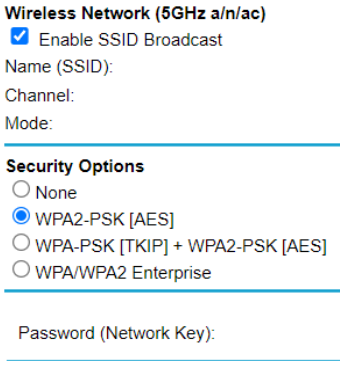
1) Guest Network Access: This feature gives a separate network for any guests to use when visiting our home through their website.

2) Firmware Updates: This feature allows the software inside our router to be caught up with what NETGEAR has updated the firmware through their website (even though we currently are not).

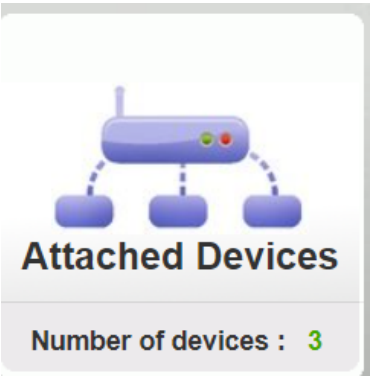


3) WiFi Protected Access (WPA): This feature is a setting that allows us to choose

the preset option that works best for our router through their website.



4) VPN Support: This feature allows us to connect several devices all at once to a singular network, protecting them with a secure connection.



5) Parental Controls: This feature allows the admin to control when the wifi should turn on and off during certain times of the day through their website (although we are currently not using this feature).

* Note: Below are some resources I used to help me with this assignment.

- Goodrich & Tamassia, Introduction to Computer Security, Addison Wesley, 2011 (Textbook)
- L02b-Ch01-CIA PowerPoint (Slides)
- What is Cryptographic Hash? - TechJury (to better understand crypto hash)
- NETGEAR AC1750 Smart WiFi Router Model R6400 (Router Box)