

**CSCI 310, Cybersecurity**

**Assignment#5**

# Q1. Multiple Choice Questions (20 points – 2 points each)

1. A(n) \_\_\_\_\_\_\_\_\_\_\_\_ is any input (i.e., a piece of software, an argument string, or sequence of commands) that takes advantage of a bug, glitch or vulnerability in order to cause an attack.

* 1. risk
  2. threat
  3. exploit
  4. control

1. In the Tim Lloyd logic bomb attack on Omega Engineering, what type of vulnerability was the existence of the user, “12345,” an example of?

* 1. rabbit
  2. backdoor
  3. virus
  4. logic bomb

1. A file owner wanted to grant full permissions for himself on the file: myfile.ext, read only for his group and he wanted to forbid everyone else from accessing the file. The correct symbolic notation for the file permissions is

* 1. - rwx-op-xx
  2. - rnor--xxx
  3. - rwxr-----
  4. - r--rwx—x

1. A file owner wanted to change file permissions to a file so that the new permissions would allow the file owner to read and execute, and **deny** anybody else all access. The correct new permissions on the file in octal notation would be

* + 1. 0400
    2. 0644
    3. 0500
    4. 0570

1. In cyber risk management, \_\_\_\_\_\_\_ the risk by buying a cyber insurance policy is considered as a risk response when considering risk scenarios where investment in security controls is very high.

* + 1. Accepting
    2. Mitigating
    3. Avoiding
    4. Transferring

1. A(n) \_\_\_\_\_\_\_\_\_ attack is an attack on a computer system or network that causes a loss of service to users.

* + 1. DDoS
    2. spam
    3. logic bomb
    4. stealth

1. A(n) \_\_\_\_\_\_\_\_\_\_ virus is a virus that mutates with every infection by adding padding code, making detection by the "signature" of the virus impossible.

* + 1. encrypted
    2. polymorphic
    3. stealth
    4. metamorphic

1. When analyzing cyber attacks, a cyber analyst could use \_\_\_\_\_\_\_\_\_\_ to understand the different stages of the cyber attack and to map used tactics and techniques.

* 1. NIST Cybersecurity Framework
  2. IRAM Risk Management Framework
  3. MITRE ATT&CK Framework
  4. NERC CIP

1. In the Needham-Schroeder With Denning-Sacco Modification Key exchange protocol, adding

\_\_\_\_\_\_\_\_\_\_\_\_\_ can prevent

* 1. Replay attacks in first step
  2. Eve impersonating Alice in conversation with Cathy
  3. Replay attacks in third step
  4. Eve impersonating Bob in response to Alice

1. When using public key cryptography, to establish the goal of non-repudiation, the plain-text message from the sender is encrypted using:
   1. Recipient’s public key
   2. Sender’s public key and a shared secret key
   3. Recipient’s private key
   4. Sender’s private key

# Q2. Short Answer Questions (40 points – 4 points each)

1. Suppose N users. For all-pair communications, (i) how many keys are required for symmetric encryption, and (ii) how many keys are required for asymmetric encryption? All-pair communication means that every user should be able to communicate with all other N-1 users in the N group.

1. Suppose Alice and Bob communicate using public key encryption. (i) Alice wants to send a message to Bob in a **confidential** way, then which key should be used for encrypting this message? (ii) Now, Alice wants to send a **signed contract** document to Bob. Which key should be used for signing digitally?

1. Suppose 4-digit PIN numbers (i.e., 0000 – 9999) for an ATM machine. How long, on average, would it take an attacker to guess such a PIN number if she could test one PIN number every 10 millisecond?

1. Give an example of the false sense of security that can come from using the “security by obscurity” approach.

1. Explain the principle of “attenuation of privilege” and provide an example.

1. Consider the following scenario and discuss the relevant potential cybersecurity ethical issues.

“Dev and Katia, a pair of talented freelance hackers, identify a previously unknown but easily fixed vulnerability in the current operating system of a particular manufacturer’s mobile phones, which allows the remote injection and execution of malicious code. As they discuss what they should do next—contact the affected the manufacturer via a backchannel, notify a popular tech media news site, or expose the vulnerability on their own cybersecurity blog— Dev and Katia are approached by a friend, who works for the phone manufacturer’s primary competitor. The friend offers them both lucrative jobs, on the condition that they remain silent about the exploit they have found.”

1. Explain how it would give a potential intruder an additional advantage if he can spend a week stealthily watching the behaviors of the users on the computer he plans to attack.

1. Show the result of encrypting M = 4 using the public key (e, n) = (3, 77) in the RSA cryptosystem.

1. What are HIPAA and FERPA? And what types of records are protected by each?

1. Transparency and disclosure is one of the cybersecurity ethical issues. Expand on why it is a challenge, and what are some of the approaches proposed to address it.

1. (bonus – 10 points) List 5 cyber attacks (incidents in recent years) and for each explain the approach, mechanism, and impact?

**Q3. What is GDPR, why is it important and what are some (5) individual privacy rights that are defined under GDPR? (10 points)**

# Q4. Access Control (15 points, 5 points each)

Consider the following access privileges. Assume the owner of a file has all of read, write, and execute privileges.

i) Alice is the owner of “GoldenGate.jpg” and “TripPlanner.exe” ii) Bob is the owner of “DFW.jpg”, “AllenOutlet.doc”, and “ReviewSite.exe” iii) Charlie is the owner of “LikeYelp.exe” iv) Charlie has read access right to all the image files (i.e., jpg). v) Bob can read and execute any executable files (i.e., exe).

Answer the following questions.

1. Construct an access control matrix (sparse matrix).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

1. Construct a capability list.

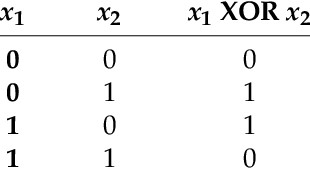
1. Construct an access control list.

**Q5. Key Exchange (15 points)**

Alice and Bob shared an n-bit secret key some time ago. Now they are no longer sure they still have the same key. Thus, they use the following method to communicate with each other over an insecure channel to verify that the key K\_A held by Alice is the same as the key K\_B held by Bob. Their goal is to prevent an attacker from learning the secret key.

* + 1. Alice generates a random n-bit value R.
    2. Alice computes X = K\_A R, where  denotes the exclusive-or boolean function, and sends X to Bob.
    3. Bob computes Y = K\_B  X and sends Y to Alice.
    4. Alice compares R and Y . If R = Y , she concludes that K\_A = K\_B, that is, she and Bob have indeed the same secret key.

Recall the XOR truth table shown below:



* 1. Draw the key exchange interaction diagram and use the syntax we studied in class to tag each of the steps

* 1. Argue how the proposed method would actually achieve their objectives.

* 1. Show how an attacker eavesdropping the channel can gain possession of the shared secret key.