1. Answer the following questions about malicious logic.

Write down the names of any 5 types of viruses.

What is hoax? In what ways is it like a worm?

Consider the following example of rabbit:

While true

Mkdir x(create a directory named x)

Chdir x(make the newly created directory the current directory)

Done

Would this still be a rabbit if you removed the chdir x? Explain.

1. Explain in short difference betw’n authentication and authorization.
2. What are backdoors and how do they differ from torjan horses?
3. Answer in short the following questions related to DMZ.

(a). What is DMZ?

(b). List the four DMZ servers and briefly describe their primary function and responsibilities in the Drib network.

(c). Briefly explain how the principle of least privilege has been followed by each of the servers in the DMZ.

5. The Following questions are related with evil user input.

a. What is buffer overflow?

b. How does JVM prevent overflow?

c. Is a java application which runs on JVM immune from buffer overflow?

6. Answer the following questions related with cross-site scripting.

a. What is XSS?

b. Give example of how XSS could happened and what problem it could cause.

c. How to prevent XSS?

7. Complete the following Drib systems ACM. You need to show how the user classes are accessing the data classes. Fill with r for read, w for write.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | PD | DEP | DDEP | CpD | CuD |
| Outsiders |  |  |  |  |  |
| Developers |  |  |  |  |  |
| Corporate |  |  |  |  |  |
| Employees |  |  |  |  |  |

|  |  |
| --- | --- |
| PD | Public Data |
| DDEP | Development data for existing products |
| DDEP | Development data for future products |
| CpD | Corporate data |
| CuD | Customer data |

8. Briefly describe the conflict betw’n the principle of economy of mechanism and the principle of psychological acceptability. By Conflict I mean that it is sometimes difficult to satisfy both principles at the same time. Try to explain it with an example.

9. Consider the following security policy and mechanism in a soccer match. Policy: no one is allowed into the stadium unless they have purchased a ticket. Mechanism: security guards are posted in the stadium; usher check tickets when the fan enters the stadium; when the fan enters, the turnstiles keep an automatic count of the number of fans who entered.

Give example of each implementations of the three models of instruction detection models for above scenario.

10. Briefly explain any 2 of your favorite SCI points that you’ve learned in this course so far.

11. The following questions are related with asymmetric cryptography, digital signature and hash/checksum. Be clear about the key(Alice’s public/private key or Bob’s public/private key). 10

a. Which key does Alice need to use to digitally sign a document for Bob?

b. Which key does Alice need to use to encrypt a document for Bob?

c. Which key does Bob need to use to decrypt a document from Alice?

d. Is it okay for Alice to share her private key to others? Why? Give brief explanations.

e. Can I generate hash/checksum of a document using private or public key? Why? Give brief explanations.

12. Write down 3 goals of intrusion detection systems.

13. What are three models of intrusion detection. Explain each model briefly.

14. In Bell­LaPadula model, the security levels are TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories are A, B, and C. Specify what type of access (read, write, both, or neither) is allowed in each of the following situations. Also briefly explain your answer. Assume that discretionary access controls allow anyone access unless otherwise specified. a) [3] Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, {B}). **WRITE**

b) [3] Paul, cleared for (TOP SECRET, {A, C}), wants to access a document classified (SECRET, {B, C}).

c) [3] Sammi, cleared for (TOP SECRET, {A, C}), wants to access a document classified (CONFIDENTIAL, {A}).

d) Anna, Cleared for (CONFIDENTIAL,{C}), wants to access adocument classified {CONFIDIENTIAL,{B}). **NEITHER**

e) Jesse, cleared for (SECRET,{C}), wants to access a document classified (CONFIDIENTIAL,{C}). **READ**

15. Policy restricts the use of electronic mail on a particular system to faculty and staff. Students can’t send or receive electronic mail on that host. Classify the following mechanisms as secure, precise, or broad and briefly justify your answer.

a. The electronic mail sending and receiving programs are disabled. **SECURE**

b. As each letter is sent or received, the system looks up the sender in a database. If party is listed as faculty or staff, the mail is processed. Otherwise, it is rejected. **PRECISE**

c. The electronic mail sending programs ask the user if he or she is a student. IF so, the mail is refused. The electronic mail reciving programs are disabled. **BROAD**

16. Alice wants to send a large message M to Bob by maintaining the integrity of the message. She also wants to assure Bob that the message indeed came from her. How would she do that? (hint: Think about digitals signatures)

17. What are the 3 different servers used in Kerberos. Briefly explain their roles in this protocol?

18. Briefly explain any 3 ways by which a Trudy can compromise the verification of certification.

19. Suppose that you are given a task to design an authentication system based on password. What suggestions would you give the user to choose strong passwords? OR write down any 3 characteristics of strong passwords.

20.Give an example of a situation in which a compromise of confidentiality leads to a compromise in integrity.

21. Let’s say that I can control some process by sending a “stop” and “start” message to a server. The fact that I am starting and stopping the process is not a secret, so I don’t have to encrypt the start and stop message. But it is important that I am the only person who can stop and start the process. Therefore. I digitally sign the “stop” or “start” message with my private key. The server then decrypts the hash with my public key to make sure that I was the one who sent the message. Briefly describe what is wrong with this protocol.

22. Consider a computer system with the three users: Alice, Bob and Cyndy. Alice owns the file Alicerc, and Bob and Cyndy can read it. Cyndy can read and write the file Bobrc, which Bob owns, but Alice can only read it. Only Cyndy can read and write the file Cyndyrc, which she owns. Assume the owner of each of these file can execute it. Create the corresponding access control matrix.

23. A cryptographe once stated that cryptography could provide complete secutiry and that any other computer security controls were unnecessary. Why is he wrong? (Hint: Think of an implementation of a cryptosystem, and ask yourself what aspects of the implementation can cryptography not protect).

24. The Clark Wilson integrity model supports (Principle of separation of privilege). Please Justofy your answer.

25. Let eCA be the public key of a CA, dCA be the private key of that CA and eJack be the public key of Jack. How would a certificate issued by CA for Jack look like?

26. a. **Vulnerabilities** are weaknesses in the systems that allow an attacker to carry out a threat.

b. **Chinese Wall Model** is a model of security policy that refers equally to confidentiality and integrity, and deals with conflict of interest.

c. In an ACM, only allowed permissions are shown. A bank square in the ACM means that the associated process has no permissions on the associated object. This follows the principle of **fail-sale defaults.**

27. What is digital signature?