DDWC 3343 / DDWD 3343

COMPUTER SECURITY

Name: DAYANG NUR NAZIHAH BINTI M ROSLAN

Matric No: A22DW0255

Instruction: Answer all questions. If plagiarism detected, you will be penalty. Please complete this assessment using your brain. Thank you ��

1. Brief overview of the importance of encryption in computer security. [5 marks]
   - Data confidentiality: encryption ensures that sensitive information such as personal data and financial details are inaccessible to unauthorized users
   - Data integrity: by preventing unauthorized modifications to the data. All changes can be detected throughout the process
   - Authentication: verify the identity of user and system through digital signatrues and certificates to verify source
2. List and explain **THREE (3)** different of malicious and non-malicious code [6 marks]

MALICIOUS	ASPECT	NON-MALICIOUS
Software that is intentionally created to cause harm, steal information or disrupt operations	design	Code that was created not with harmful intent but can cause security vulnerabilities
Planted by individual or hacker with intent to destruct	reason	Most likely due to human error or incompetence in structuring the code
Virus, worm, trojan	examples	Insecure code, unhandled exceptions

3. Explain the concept of cryptography and list **THREE (3)** its relevance in today's digital world.[5marks]

Cryptography is the art of using encryption to conceal text. Its relevance is by playing a vital role in computer security by ensuring three aspects:

- Confidentiality: authorized parties only can access/understand the message
- Integrity: data cannot be altered without detection
- Authentication: verifies the identities of the parties involved in communication

4. List **FOUR (4)** method to detect the virus.

- Detect by virus signature
- Track storage pattern
- Execution patterns
- Transmission patterns

5. Imagine, you own a company that need to do money transaction every day. [10 marks]

   a. List **FOUR (4)** threat and how to overcome each threat.

      - Phishing attacks

        How to overcome: implement required employee training to recognize threats through emails and use encrypted emailing services and filtering solutions.

      - DDoS Attacks

        How to overcome: use protection services across the company while increasing the network bandwidth capacity.

      - Ransomware

        How to overcome: use anti-malware software while regularly conduct system updates and strengthen the security walls

   - Man in the Middle Attacks

     How to Overcome: use strong encryption protocols for all transactions
     and use VPNs on the computer systems.

   b. Explain the mechanism that will be implemented to protect and secured user personal data to prevent data breaches.

      Encryption – encrypt data during transit and when it is being stored on the servers to ensure that even if attackers were to gain access to the data, they would not be able to read it without using the proper decryption keys.

6. In the context of computer security, explain the **TWO (2)** difference between symmetric and asymmetric encryption. [4 marks]

Symmetric	Aspect	Asymmetric
Uses a single key for encryption and decryption	Key usage	Uses two keys for encryption and decryption (public and private)
Faster because less complex due to one key usage	Speed	Requires more time as it is more complex with two keys, suitable for small data

7. Discuss **TWO (2)** advantages and disadvantages of each symmetric and asymmetric encryption method in ensuring data confidentiality and integrity. [4 marks]

Method	Advantage	Disadvantage
Symmetric	Faster and more efficient for large data	Failure risk – if key is compromise, all data is risked
	Easier to implement	Less secure due to shorter key lengths
Asymmetric	Non-repudiation	More complex to set up and manage
	Solves key distribution problem with public and private keys	Higher resource usage which is not ideal for larger datasets

8. Provide **TWO (2)** examples of where each type of encryption might be used in real-world applications. [2 marks]

Symmetric: File encryption

Asymmetric: email encryption