DDWD 3343 COMPUTER SECURITY
MISS SITI FATIMAH BTE MOHAMAD AYOP

UTM UNIVERSITI TEKNOLOGI MALAYSIA | Sekolah Pendidikan Profesional dan Pendidikan Berterusan (SPACE)

INDIVIDUAL ASSIGNMENT 1

COURSE CODE : DDWD 3343
COURSE NAME : COMPUTER SECURITY
YEAR / PROGRAMME : 3 DDWD
SUBMISSION :

INSTRUCTION / *ARAHAN:*

1. THIS ASSESSMENT WILL CONTRIBUTE 5% OF THE ASSESSMENT.
2. PLEASE SUBMIT THIS LAB SKILL IN FORM OF PDF (SOFTCOPY) / A4 PAPER SIZE (HARDCOPY) BEFORE **15 SEPTEMBER 2024.**
3. MAKE SURE TO COMPLETE ALL ASSESSMENT
4. PLEASE FOLLOW THE FORMAT:
    a. TIMES NEW ROMAN FONT SIZE 12.
    b. SPACING 1.5.
    c. JUSTIFY ALIGNMENT THE PARAGRAPH.
5. THE FAILURE FOLLOWING THE REQUIREMENT WILL CAUSE LOSING MARK
6. PLEASE FOLLOW THE RUBRIC ASSESSMENT:

CRITERIA	**4POINTS**	**3POINTS**	**2POINTS**	**1POINTS**
SUBMISSION FORMAT **[/4]**	FOLLOW ALL FORMAT INSTRUCTION	DID NOT FOLLOW 1-2 OF THE FORMATS	DID NOT FOLLOW 2-3 OF THE FORMATS	NOT MAINTAINING THE TIDY OF THE TASK
UNDERSTANDNG VALUE **[/4]**	ABLE TO UNDERSTAND THE BASIC CONCEPT OF SECURITY, GIVING EXAMPLE AND RELATE TO THE THREAT BY EXLAINING HOW TO SOLVE THE PROBLEM	ABLE TO UNDERSTAND THE BASIC CONCEPT OF SECURITY, GIVING EXAMPLE AND RELATE TO THE THREAT AND HOW TO SOLVE THE PROBLEM	ABLE TO UNDERSTAND THE BASIC CONCEPT OF SECURITY, GIVING EXAMPLE THAT RELATE TO THE TOPIC.	ABLE TO UNDERSTAND THE BASIC CONCEPT OF SECURITY AND LIST THE EXAMPLE.

DDWD 3343 COMPUTER SECURITY
MISS SITI FATIMAH BTE MOHAMAD AYOP

ANSWER ELABORATION **[/4]**	STUDENT ABLE TO ANSWER ALL QUESTION GIVEN, DISCUSS AND ELABORATE THE ISSUE, RELATE TO THE CURRENT SITUATION, AND COMPARE TO OTHER ALTERNATIVE SOLUTION OR ISSUE.	STUDENT ABLE TO ANSWER ALL QUESTION GIVEN STUDENT ABLE TO ELABORATE THE ISSUE, RELATE TO THE CURRENT SITUATION, AND COMPARE TO OTHER ALTERNATIVE SOLUTION OR ISSUE.	STUDENT ABLE TO ANSWER ALL QUESTION GIVEN, ELABORATE THE ISSUE, RELATE TO THE CURRENT SITUATION, AND LIST TO OTHER ALTERNATIVE SOLUTION OR ISSUE.	STUDENT ABLE TO ANSWER ALL QUESTION GIVEN ELABORATE THE ISSUE, AND LIST TO OTHER ALTERNATIVE SOLUTION OR ISSUE.
EXAMPLE PROVIDE AND DISCUSSION **[/4]**	STUDENT ABLE TO LIST AT LEAST 2 EXAMPLE THAT CONTAINS PRO AND CONS OF THE SITUATION, EXPLAIN THE EXAMPLE THAT RELATE TO THE CURRENT SITUATION.	STUDENT ABLE TO LIST AT LEAST 2 EXAMPLE THAT CONTAINS PRO AND CONS OF THE SITUATION AND EXPLAIN THE EXAMPLE.	STUDENT ABLE TO LIST 1 EXAMPLE THAT CONTAINS PRO AND CONS OF THE SITUATION AND EXPLAIN THE EXAMPLE.	STUDENT ABLE TO LIST 1 EXAMPLE THAT CONTAINS PRO AND CONS OF THE SITUATION
PLAGIARISM **[/4]**	NO PLAGIARISM DETECT (ORIGINALLY FORM STUDENT)	1- 20% PLAGIARISM DETECTED	21-50% PLAGIARISM DETECTED	>50% PLAGIARISM

STUDENT NAME:	DAYANG NUR NAZIHAH BINTI M ROSLAN
MATRIC NUMBER:	A22DW0255

INSTRUCTION: ANSWER ALL QUESTIONS

CHAPTER 1:

1. Define what is computer security.
2. List and explain important terminologies in computer security.
3. List and discuss threats with regard to computer security.
4. Understand what are security vulnerabilities.
5. Explain security principles (goals).
6. Discuss security strategies and controls.

CHAPTER 2:

1. Explain cryptography and its importance in computer security.
2. Describe cryptosystem, and encryption / decryption process.
3. Differentiate between symmetric and asymmetric cryptosystem.

4. List and explain **THREE (3)** various encryption/ decryption algorithms.
5. Cryptography:
    a. Solve encryption for message: “Malaysia Madani” and key: “c” using ceaser cipher.
    b. Solve encryption for message: “Computer Security” and key: “begin” using vernam cipher.
    c. Solve encryption for message: “Saya Sayang Miss Fatimah” and key: “iyelatu” using columnar transposition cipher.
6. Discuss and list the **STRENGTH** and the **WEAKNESS** of each encryption method.
7. Given p=23 and q= 17, encrypted message = 11 using RIvest Shamir Adelman (RSA) algorithm.
8. Given p=27 and g=13, using Diffie Hilam Algorithm, solve:
    a. Private key for Ilyas, given public key = 9.
    b. Private key for Ibrahim, given public key = 7.
    c. Find share key.

CHAPTER 3:

1. Define the concept of secured program.
2. Differentiate malicious and non-malicious code.
3. Identify and describe programming errors with security implication.
4. List and explain different types of viruses, how and where it attacks and how it gains controls.
5. Explain virus signature.
6. Identify the impact of viruses to the computing system.
7. Discuss and explain various policies, procedures and technical controls against virus threats.

CHAPTER 1

INTRODUCTION

1.1 Introduction

Computer security involves safeguarding computers, their associated data, networks, software and hardware from unauthorized access, misuse, theft, information loss, and various security threats. While the internet has greatly simplified our lives and offered numerous benefits, it has also exposed our systems to risks such as viruses, hacking, data theft, and potential damage to the system. The basic guideline for computer security is CIA.

1. Confidentiality: ensures that computer related assets are accessed only by authorized parties.
2. Integrity: assets can be modified only by authorized parties or by authorized ways.
3. Availability: accessible to authorized parties at appropriate times.

1.2 Important Terminologies

Terminologies	**Explanation**
Computer System or Assets	Hardware, software, data, people
Exposure	A form of possible loss or harm
Vulnerability	A weakness in the system that can be exploited
Threat	Potentiality for loss or harm during human attacks, natural disasters, errors
Attack	Realization of a threat
Control	A protective measure/action/procedure to remove or reduce a vulnerability
Unauthorized access	Accessing a server or website using someone else's account details
Antivirus or Antimalware	A software that operates on different OS which is used to prevent from malicious software

1.3 Threats regarding computer security

1.3.1 Interception

A type of security threat when an unauthorized party gains access to an asset or computer system. Some examples are wiretapping, illicit copying programs or files, capturing information during transmission and so on and so forth. This happens without the knowledge of the subject involved.

Sensitive information such as login credentials, personal data can be stolen during an interception as their privacy is breached. This can lead to identity theft, reputational damage and legal consequences. Issues in data integrity can also arise as intercepted data can be altered before it reaches its destination.

How does interception occur? One of the ways is attackers would use tools knows as sniffers to monitor and capture data that travels over a network. Unencrypted data that are being transmitted over devices are the most vulnerable assets.

1.3.2 Interruption

A type of security threat where an asset or service becomes unavailable or unusable due to unauthorized access. An attacker would disrupt the normal function of a system, preventing legitimate users from accessing resources or services they need.

Legitimate users are blocked from accessing critical resources, which can halt business operations, delay services, and cause financial loss.

How does interruption occur? A common method is through Distributed Denial of Service (DDoS). DDoS is when malware is turned into a network of interconnected devices called botnets. These botnets are tasked to send false request that disrupts the traffic of a server. The server is needs to filter out which makes normal traffic denied of service.

1.3.3 Modification

A type of security threat where changes are made to an asset or system, altering the original data or functionality. In this type or attack, an intruder gains access to a system and changer critical information, affecting its integrity and reliability. From altering files, configurations, to disruption communications between systems.

A common example is Man-in-the-Middle (MitM) attack, where an attacker intercepts and modifies data being exchanged between two parties. This can result in corrupted data, unauthorize transactions, or even the introduction of further vulnerabilities into the system. Modification attacks can lead to compromised data integrity, system malfunctions and loss of user trust, making them a serious threat to both individuals and organizations.

1.4 Security vulnerabilities

Asset	Vulnerabilities	Result	Method	Additional
Hardware	Destroyed (deleted)	Information leak	Keystroke	
Software	Stolen (pirated) Altered (but still running)		Logic bomb, trojan horse, virus, trapdoor	
Data				Fabricated data

1.5 Security Principles (Goals)

Security Principle	**Description**
Confidentiality	- Only authorized recipients can access the contents of an encrypted message. - Ensures that computer-related assets are accessed only by authorized parties. - Prevents improper disclosure of information.
Integrity	- Ensures that the recipient can determine if the message has been altered during transmission.
Availability	- Ensures that the recipient can identify the sender and verify that the purported sender actually sent the message.
Accountability	- Ability to map actions within a system to responsible parties. - Prevents improper use of resources.

Access Control	- Specifies and controls who can access specific resources.
Authentication	- Identifies the user of the computer system and builds trust with the recipient.
Non-Repudiation	- Ensures that the sender of a message cannot deny having sent the message.

1.6 Security Strategies and Controls

Security Measure	**Description**	**Example 1 – Private Property**	**Example 2 – E-Commerce**
Prevention	Take measures to prevent assets from being damaged.	- Lock door, window	- Encrypt orders
Detection	Take measures to detect when, how, and by whom an asset has been affected.	- Missing item, alarm sounding	- Unauthorized transaction appears
Reaction	Recover assets or recover from damage to assets.	- Call police, claim insurance	- Complain, discontinue card, get a new card

CHAPTER 2

CRYPTOGRAPHY

2.1 Introduction

Cryptography – the practice (or art) of using encryption to conceal text. It plays a vital role in computer security by ensuring:

- Confidentiality: Only authorized parties can understand the message.
- Integrity: The data cannot be altered without detection.
- Authentication: Verifies the identities of the parties involved in communication.
- Non-repudiation: Prevents denial of sending or receiving the data.

2.2 Cryptosystem and its process

A cryptosystem is a framework consisting of algorithms for encryption and decryption, keys, and key management processes used for secure communication.

- Encryption: The process of converting plain text into ciphertext using an algorithm and a key, making it unreadable to unauthorized users.
- Decryption: The process of converting ciphertext back into its original plain text form using a key, allowing authorized users to read it.

2.3 Symmetric and asymmetric cryptosystem

Aspect	**Symmetric Cryptosystem**	**Asymmetric Cryptosystem**
Key Usage	Same key for both encryption and decryption	Pair of keys: public key for encryption, private key for decryption
Speed	Faster and more efficient, especially for large data	Slower due to complex calculations
Security	Less secure; requires secure key distribution	More secure; public key can be shared openly
Common Algorithms	AES, DES, 3DES	RSA, ECC (Elliptic Curve Cryptography)
Typical Use Cases	Bulk data encryption, real-time applications	Digital signatures, secure key exchange

Key Management	Challenging, as the same key must be shared securely	Easier, as only the private key must be kept secret

2.4 Algorithms

1. AES (Advanced Encryption Standard):

   AES is a widely adopted symmetric encryption algorithm known for its security and efficiency. It encrypts data in fixed 128-bit blocks using key sizes of 128, 192, or 256 bits. AES provides robust encryption for a variety of applications, including secure communications, data protection, and online transactions. Its balance of security and speed makes it suitable for both software and hardware use, and it is trusted by governments and industries worldwide.

2. RSA (Rivest-Shamir-Adleman):

   RSA is an asymmetric encryption algorithm that uses two keys: a public key for encryption and a private key for decryption. It relies on the difficulty of factoring large prime numbers, providing secure data transmission. RSA is commonly used in digital signatures, secure key exchanges, and protecting sensitive information over the internet. Though slower than symmetric algorithms, RSA is highly secure and foundational in modern encryption systems.

3. DES (Data Encryption Standard):

   DES is a symmetric encryption algorithm that encrypts data in 64-bit blocks using a 56-bit key. Once widely used, DES has become outdated due to vulnerabilities from its shorter key length, making it susceptible to brute-force attacks. However, it was pivotal in the development of more secure algorithms, like AES, and is still referenced in cryptography history.

2.5Cryptography solution

a. Malaysia Madani – Caesar (key=c)

M	A	L	A	Y	S	I	A		M	A	D	A	N	I
12	0	11	0	24	18	8	0		12	0	3	0	13	8
14	2	13	2	26	20	10	2		14	2	5	2	15	10
				1										
o	c	n	c	b	u	k	c		o	c	f	c	p	k

=Ocncbukc Ocfcpk

b. Computer security – Vernam (key=begin)

	b	e	g	i	n
	1	4	6	8	13

DDWD 3343 COMPUTER SECURITY
MISS SITI FATIMAH BTE MOHAMAD AYOP

C	O	M	P	U	T	E	R
2	14	12	15	20	19	4	17
1	4	6	8	13	1	4	6
3	18	18	23	33	20	8	23
				8			
3	18	18	23	8	20	8	23
D	S	S	X	I	U	I	X

S	E	C	U	R	I	T	Y
18	4	2	20	17	8	19	24
1	4	6	8	13	1	4	6
19	8	8	28	30	9	23	30
			3	5			5
19	8	8	3	5	9	23	5
T	I	I	D	F	J	X	F

c. Saya Sayang Miss Fatimah – columnar transposition (key=iyelatu)

3	7	2	4	1	5	6
I	Y	E	L	A	T	U
S	A	Y	A	X	X	X

= AXEYISLATXUXYA

3	7	2	4	1	5	6
I	Y	E	L	A	T	U
S	A	Y	A	N	G	X

=ANEYISLATGUXYA

3	7	2	4	1	5	6
I	Y	E	L	A	T	U
M	I	S	S	X	X	X

=AXESIMLSTXUXYI

3	7	2	4	1	5	6
I	Y	E	L	A	T	U
F	A	T	I	M	A	H

=AMETIFLITAUHYA

2.6 Strength and weakness

Encryption Method	Strengths	Weaknesses
Caesar Cipher	Simple and fast	Easily broken by frequency analysis
Vernam Cipher	Perfect security if used with a truly random key (one-time pad)	Difficult key management; requires key as long as the message
Columnar Transposition	Fairly strong against brute force if the key is complex	Vulnerable to pattern recognition and plaintext attacks if the key is short

2.7RSA

p = 23

q = 17

n = p x q

= 23 x 17

=391

$\phi(n)=(p-1)\cdot(q-1)$

$\phi(n)=(23-1)\cdot(17-1)$

$\phi(n)=352$

e = {3,5,7…}

1 × 352

2 × 176

4 × 88

8 × 44

11 × 32

16 × 22

d = 1+k(ϕn) / e

K=0

= 1/3

K=1

=353/3

K=2

=235 d=235

Encrypted message (c) = 11

Decrypted message (m) = 11^235 mod 391 = 148

2.8Diffie-Hellman

p=27 g = 13

Ilyas(A) = 9, Ibrahim(B) = 7

x = g ^ A mod p
= 13 ^ 9 mod 27
=1

y = g^B mod p
= 13^7 mod 27
= 4

z1 = B ^ x mod p
= 4 ^ 9 mod 27
= 1

z2 = B ^ x mod p
= 1^7 mod 27
= 1

Shared key = 1, z1 = z2

CHAPTER 3

PROGRAM SECURITY

3.1 Secured program concept

A secured program is designed and implemented to prevent unauthorized access, manipulation, or damage to data and systems. It includes features such as authentication, encryption, and input validation to protect against vulnerabilities and attacks like data breaches, malware, or system crashes.

3.2Malicious code

Type	Description	Examples
Malicious Code	Software or scripts intentionally created to cause harm, steal information, or disrupt operations.	Viruses, Worms, Trojans, Ransomware
Non-malicious Code	Code not created with harmful intent but may still cause security vulnerabilities if poorly written (e.g., insecure code, unhandled exceptions).	Insecure code, unhandled exceptions

3.3Programming errors

1. Buffer Overflows:
- Occurs when a program writes more data to a buffer than it can hold.
- Leads to data overwriting adjacent memory, causing potential execution of arbitrary code.
- Attackers can exploit this vulnerability to gain control over the system.
2. Incomplete Mediation:
- Happens when user inputs or data are not properly validated or sanitized.

- Can result in injection attacks (e.g., SQL Injection, Cross-Site Scripting).
- Allows attackers to manipulate data or gain unauthorized access.

3. Time-of-Check to Time-of-Use (TOCTOU) Errors:

- Arises when there's a delay between validation and the actual use of a resource.
- Attackers can exploit this timing gap to modify the resource after validation.
- Can result in privilege escalation or system compromise.

4. Combination of Non-malicious Program Flaws:

- Minor flaws (e.g., poor exception handling, insecure configurations) may seem harmless individually.
- When combined, these flaws create vulnerabilities that attackers can exploit.
- Insecure handling of sensitive data or weak encryption practices can expose systems to threats.

3.4Virus

Type of Virus	**How They Attack**	**Where They Attack**	**How They Gain Control**
Appended Virus	Attaches to the end of executable files.	Program files (e.g., .exe, .com).	Replaces or appends itself to the host file.
Surrounding Virus	Wraps around the executable, modifying both start and end.	Program files.	Gains control by executing before and after the host program.
Integrated Virus	Replaces entire code of a program with its own.	System files, critical applications.	Fully integrates itself and replaces the original program.
Document Virus (Macros)	Infects documents with embedded macro code.	Document files (e.g., Word, Excel).	Executes macros automatically when the document is opened.
Boot Sector Virus	Infects the boot sector of storage media (e.g., hard disks).	Boot sector.	Gains control during system startup before the OS loads.
Memory Resident Virus	Loads into memory and stays active even after infected programs are closed.	RAM (memory).	Remains in memory, infecting files and programs running on the system.

Polymorphic Virus	Alters its code to evade detection.	System files, program files.	Constantly changes its appearance, making it harder for antivirus to detect.
Ransomware	Encrypts user files and demands payment for decryption.	User files, databases.	Gains control by encrypting files and locking the user out until ransom is paid.

3.5 Virus signature

A virus signature is a unique pattern or sequence of bytes that identifies a particular virus or malware. Antivirus software uses virus signatures to detect known viruses by comparing files and programs against its database of known signatures.

3.6 Impact

1. Data Loss - Erasure or corruption of files leading to permanent loss of important data.
2. System Performance Issues - Sluggish performance or crashes due to excessive resource consumption by viruses.
3. Unauthorized Access - Potential breaches of sensitive information through unauthorized control gained by certain viruses.
4. Financial Costs - Expenses for system repairs, replacements, and downtime resulting from virus infections.

3.7 Control against virus threats

Category	**Policy/Procedure/Control**	**Description**
Developmental Controls	**Modularity**	Break down tasks into subtasks to manage complexity and enhance development.
	Encapsulation and Information Hiding	Hide implementation details of components, treating them as "black boxes" with defined inputs and outputs.
	Peer Reviews	Conduct formal reviews, walkthroughs, and

		inspections to identify and address errors.
	Hazard Analysis	Use systematic techniques to uncover and mitigate potential system hazards.
	Testing	Focus on making the product failure-free or tolerant, and handle faults to minimize disruption.
	Prediction	Anticipate and prepare for unwanted events to minimize their impact.
	Static Analysis	Examine design aspects such as control flow and data structure for robustness.
	Configuration Management	Control changes during development and maintenance to ensure system integrity.
	Lessons from Mistakes	Document decisions and learn from errors to prevent recurrence.
Operating Systems Controls	**Trusted Software**	Use software with rigorous development and analysis to ensure reliability and security.
	Mutual Suspicion	Assume other programs may be malicious or incorrect to enhance security.
	Access Logs	Maintain logs of access to system resources to detect unauthorized access.

	Confinement	Limit software to necessary system resources to reduce potential damage.
Administrative Controls	**Standards of Program Development**	Establish standards to guarantee correctness, quality, and security of programs.
	Separation of Duties	Focus individuals on specific tasks to reduce the risk of malicious or erroneous actions.