SLIATE

SLIATE

SRI LANKA INSTITUTE OF ADVANCED TECHNOLOGICAL EDUCATION

(Established in the Ministry of Higher Education, vide in Act No. 29 of 1995)

Higher National Diploma in Information Technology
Second Year, First Semester Examination – 2022
HNDIT 3062 Information and Computer Security

Instructions for Candidates:	No. of questions: 05
Answer any Four (04) Questions Only.	No. of pages : 09
Each question carries equal marks	Time : Two (**02) Hours**

Marking scheme

Question 01

I. What is Computer Security? Write examples for three types of assets. (04 Marks)

- ***Computer Security: The protection of the assets of a computer system***
  - ***Hardware: examples: Computer, Network, Devices***
  - ***Software: OS, utility software, commercial application***
  - ***Data: Documents, photos, email***

II. Describe the term Security Mechanism (04 Marks)

Security mechanisms are technical tools and techniques that are used to implement security services. A mechanism might operate by itself, or with others, to provide a particular service. Examples of common security mechanisms are as follows: Cryptography. Message digests and digital signatures.

III. Name the five major categories of security services defined in X.800 OSI security objectives (05 Marks)

Authentication

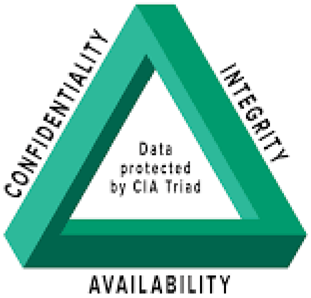
non-repudiation

access control

data integrity

data confidentiality.

IV. Briefly explain the CIA triad and its importance (06 Marks)



Confidentiality ***is roughly equivalent to privacy. Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts.***

Integrity ***involves maintaining the consistency, accuracy, and trustworthiness of data over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people***

Availability ***means information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems***

Why is the CIA triad important?

CIA each letter representing a foundational principle in cybersecurity, the importance of the CIA triad security model speaks for itself. Confidentiality, integrity and availability together are considered the three most important concepts within information security.

V. Explain Active and passive attack types (06 Marks)

Here are some common types of active attacks:

Session Hijacking Attack.

Message Modification Attack.

Masquerade Attack.

Denial-of-Service Attack.

Distributed Denial-of-Service Attack.

Trojans.

%Passive attacks are relatively scarce from a classification perspective, but can be carried out with relative ease, particularly if the traffic is not encrypted. There are two types of passive attacks: – eavesdropping (tapping): the attacker simply listens to messages exchanged by two entities.

[Total 25 Marks]

Question 02

I. Explain the differences between Cryptography and cryptanalysis (04 Marks)

Cryptography is the area of constructing cryptographic systems.

The study of encryption principles/methods

Cryptanalysis / code breaking is the area of breaking cryptographic systems.

The study of principles/ methods of deciphering cipher text without knowing key

II. List four basic properties of a good encryption algorithm. (04 Marks)

Provides high level of security (full or part of the text will not be revealed by analyzing

encrypted data. Keys will not be found)

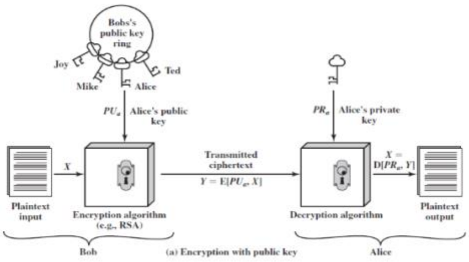
Efficient resources (memory usage etc) and time.

Economically cheep to implement as software or hardware tokens

Completely specified and is available for public access

Simple and easy to understand

III. Explain public key cryptography with a suitable diagram (05 Marks)



(a) Encryption with public key

1. Each user generates a pair of keys to be used for the encryption and decryption of messages.
2. Each user places one of the two keys in a public register or other accessible file.This is the public key.The companion key is kept private.As the previous figure suggests, each user maintains a collection of public keys obtained from others.
3. If Bob wishes to send a private message to Alice, Bob encrypts the message using Alice's public key.
4. When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice's private key.

IV. Compare and contrast between Symmetric and Asymmetric key encryption algorithms. (06 Marks)

Key Differences	***Symmetric Encryption***	***Asymmetric Encryption***
Size of cipher text	*Smaller cipher text compares to original plain text file*	*Larger cipher text compares to original plain text file*
Data size	*Used to transmit big data.*	*Used to transmit small data*

Security	*Less secured due to use a single key for encryption.*	*Much safer as two keys are involved in encryption and decryption.*
Techniques	*It is an old technique.*	*It is a modern encryption technique*
Number of keys	*Symmetric Encryption uses a single key for encryption and decryption.*	*Asymmetric Encryption uses two keys for encryption and decryption*

V. Briefly explain the following

Hash function :
condenses arbitrary message to fixed size
h = H(M)
usually assume that the hash function is public and not keyed
hash used to detect changes to message
can use in various ways with message
most often to create a digital signature

a. MAC :

generated by an algorithm that creates a small fixed-sized block
depending on both the message and some key
Like Encryption though need not be reversible
appended to the message as a ***signature***
the receiver performs the same computation on the message and checks it matches the MAC
assures that message is unaltered and comes from sender

(06 Marks)

[Total 25 Marks]

Question 03

I. Explain Authentication with 3 categories (04 Marks)

Authentication: Verification of a person's claimed identity

- *3 Categories:*
  - *What you know: Password,PIN*
  - *What you have: e-Token, Smart cards, RFID*

– *Who you are :Biometric authentication and Biometric reading*

II. Explain physical and behavioral Biometric authentication with suitable examples
Physical Biometrics: Fingerprint, Iris, DNA, Smell, Retina
Behavioral Biometrics: Signature , Voice, Keystroke, Gait

(04 Marks)

III. What is a proxy server? Write three advantages (05 Marks)

Proxy server:

Perform web retrievals on behalf of a web browser

Most often used to speed up Internet access and reduce bandwidth by caching frequently used pages

Libraries use proxy servers to make off-campus web clients look like on-campus ones

Authenticated users are allowed to relay requests through our IP address space

Advantages

Can place database links anywhere

A single URL from the database vendor

Proxy servers scale better

IV. Explain Authentication tokens with the following two examples (06 Marks)

a. X.509 certificates:

Use of digital certificates issued by a trusted Certificate Authority (e.g. VeriSign)
A Digital Certificate contains information to assert an identity claim

Name
Serial number
Expiration dates
Certificate holder's public key (used for encrypting/decrypting messages and digital signatures)
Digital signature of Certificate Authority (so recipient knows that the certificate is valid)
The recipient may confirm the identity of the sender with the Certificate Authority

b. Kerberos tickets :

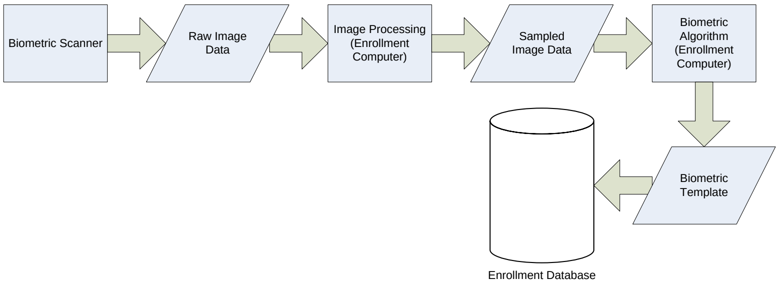
Clients share secret symmetric key with server
Clients login to authentication server
Server returns a Ticket-Granting Ticket (TGT) encrypted with client's key
Client sends decrypted TGT to Ticket Granting Service
TGS sends ticket authorizing network access and certain services
Session ticket data:

Name
Network address

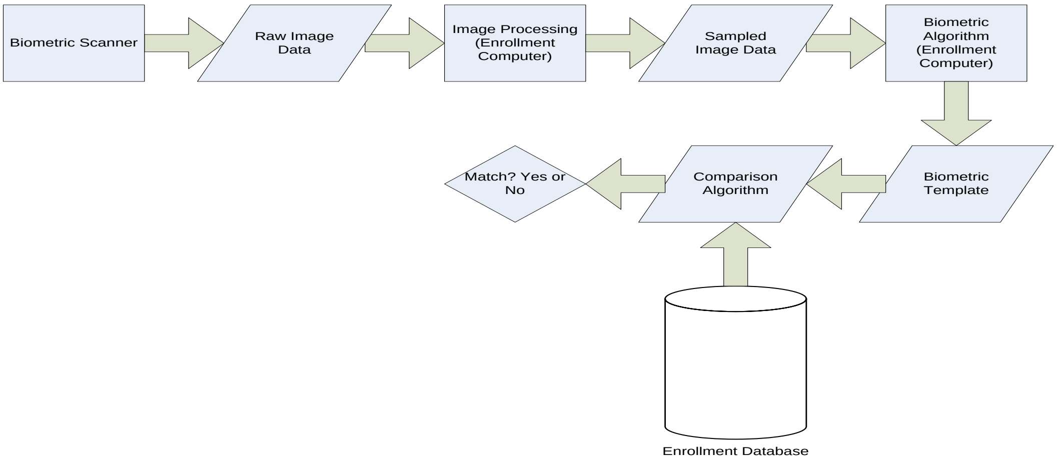
Time stamp
Expiration dates
Session key

V. Draw a flowchart and explain enrollment and verification in Biometric authentication

Enrollment:



Verification:



(06 Marks)

[Total 25 Marks]

Question 04

I. What is Access control? (04 Marks)

Granting or denying approval to use specific resources

Information system's mechanism to allow or restrict access to data or devices

II. Explain the following access control terminology (04 Marks)

a. Object

Specific resource

Example: file or hardware device

b. *Subject*

User or process functioning on behalf of a user

Example: computer user

c. *Operation*

Action taken by the subject over an object

Example: deleting a file

d. *Owner*

Person responsible for the information

III. Consider the type of virus attack and explain the following terms (05 Marks)

a. ***parasitic virus****-A Parasitic Virus (also referred to as a file virus) is a type of virus that spreads by attaching itself to another program*

b. ***memory-resident virus****-A Memory-Resident Virus is a virus that is located in the memory of a computer, even after the 'host' application or program has stopped running (been terminated).*

c. ***boot sector virus****- A boot sector virus is a type of virus that infects the boot sector of floppy disks or the primary boot record of hard disks (some infect the boot sector of the hard disk instead of the primary boot record).*

IV. Name the four services provided by a firewall for enabling network security

a. Not all firewalls offer full protection against computer viruses

b. Firewalls can't stop a hacker from masquerading as an employee

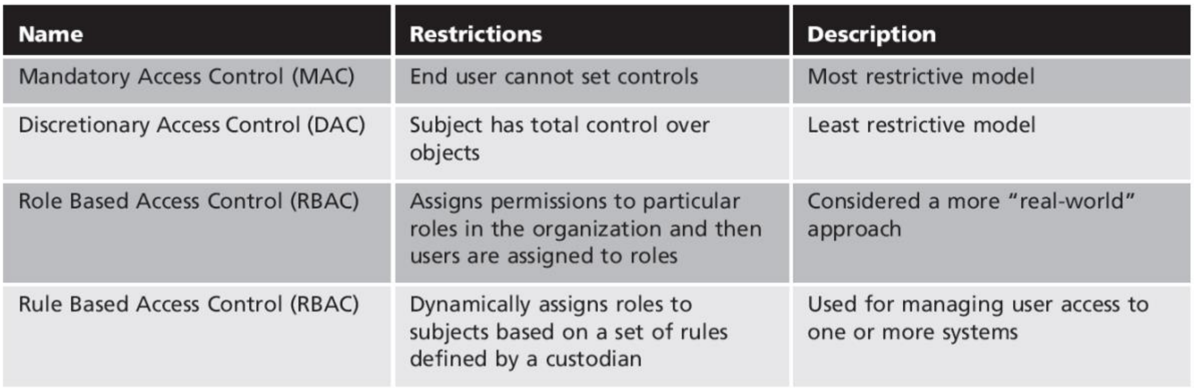
c. cannot protect from attacks bypassing it

i. eg sneaker net, utility modems, trusted organisations, trusted servic es (eg SSL/SSH)

d. cannot protect against internal threats i. eg disgruntled or colluding employees e. cannot protect against access via WLAN i. if improperly secured against external use f. cannot protect against malware imported via laptop, PDA, storage infected outside

(06 Marks)

V. Write the difference between four types of access controls (06 Marks)



Name	Restrictions	Description
Mandatory Access Control (MAC)	End user cannot set controls	Most restrictive model
Discretionary Access Control (DAC)	Subject has total control over objects	Least restrictive model
Role Based Access Control (RBAC)	Assigns permissions to particular roles in the organization and then users are assigned to roles	Considered a more "real-world" approach
Rule Based Access Control (RBAC)	Dynamically assigns roles to subjects based on a set of rules defined by a custodian	Used for managing user access to one or more systems

[Total 25 Marks]

Question 05

I. Define the following terms (04 Marks)

a. Digital certificate:
An electronic Document which provides the certification that a person is authorised to use the Public Key algorithm given to him by a trusted third party
Provided to all users of a systems when they are given the Public Key for the corresponding system
The user is bound to produce his Digital Certificate at any time on request by the employer or a customer

b. Digital Signature:
have looked at message authentication
but does not address issues of lack of trust
digital signatures provide the ability to:
verify author, date & time of signature
authenticate message contents
be verified by third parties to resolve disputes
hence include authentication function with additional capabilities

II. Write the differences between Logic Bomb and Trapdoors malicious software (04 Marks)

Trapdoors*:*
secret entry point into a program
allows those who know access bypassing usual security procedures
have been commonly used by developers
a threat when left in production programs allowing exploited by attackers
very hard to block in O/S
requires good s/w development & update

Logic Bomb:
one of oldest types of malicious software
code embedded in legitimate program
activated when specified conditions met

eg presence/absence of some file
particular date/time
particular user
when triggered typically damage system
modify/delete files/disks

III. How to prevent cross-site scripting? explain 4 methods (05 Marks)

If possible, avoiding HTML in inputs *- One very effective way to avoid persistent cross-site scripting attacks is to prevent users from posting HTML into form inputs*

Validating inputs *- Validation means implementing rules that prevent a user from posting data into a form that doesn't meet certain criteria..*

Sanitizing data - *Sanitizing data is similar to validation, but it happens after the data has already been posted to the web server, yet still before it is displayed to another user.*

Taking cookie security measures *- Web applications can also set special rules for their cookie handling that can mitigate cookie-theft via cross-site scripting attacks*

IV. Explain important three characteristics of S/MIME and PGP (06 Marks)

PGP: *widely used de facto secure email*
developed by Phil Zimmermann
selected best available crypto algs to use
integrated into a single program
available on Unix, PC, Macintosh and Amiga systems
originally free, now have commercial versions available also
S/MIME:

security enhancement to MIME email
original Internet RFC822 email was text only
MIME provided support for varying content types and multi-part messages with encoding of binary data to textual form
S/MIME added security enhancements
have S/MIME support in various modern mail agents: MS Outlook, Netscape etc

V. List three ways to secure an Email (06 Marks)

a. Use a secure email client
b. Always use text
c. Use free Webmail accounts for subscriptions and postings
d. Use additional multi-layered defenses
e. Encrypt sensitive emails

[Total 25 Marks]