CYBER SECURITY

COMPUTER SECURITY

"Measures and controls that ensure **confidentiality**, **integrity**, and **availability** of the information processed and stored by a computer"

THE CIA TRIAD					
	DEFINITION	**EXAMPLE**	**PURPOSE**	**MITIGATION**	**OPPOSITE OF CIA**
CONFIDENTIALITY	Information is safe from disclosure.	I send you a message, and no one else knows what that message is.	Data is not disclosed	Encryption	Disclosure
INTEGRITY	The information is safe from modification or alteration.	I send you a message, and you receive exactly what I send you.	Data is not tampered	Hashing	Alteration
AVAILABILITY	Information is available to authorised users when needed.	I send you a message, and you are able to receive it.	Data is available	Backups, redundant systems	Descripción

CONFIDENTIALITY

DATA CONFIDENTIALITY

Ensures confidential information, such as a student's grades, is not made available or disclosed to unauthorised individuals.

PRIVACY

Assures individuals control over what information related to them may be collected, stored and shared, e.g., data generated by smartphone

INTEGRITY

DATA INTEGRITY

Assures completeness and accuracy of data
Protection against corruption or unauthorised changes
Methods: EG: checksum, backup, version control

SYSTEM INTEGRITY

Assures a system performs its intended
function w/o deliberate manipulation.
Counterexample: compromised machine, hacked website

AVAILABILITY

Assures that systems, applications and data accessible to authorized users.

Counterexample

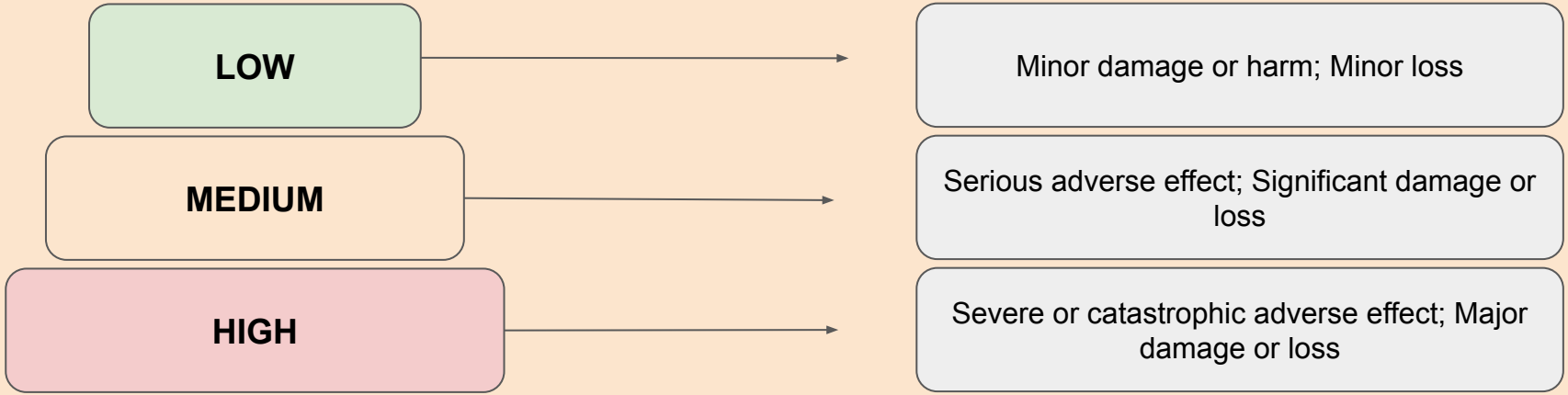
- A system under Denial of Service (DoS)
- Ransomware: criminal encrypt files for ransom

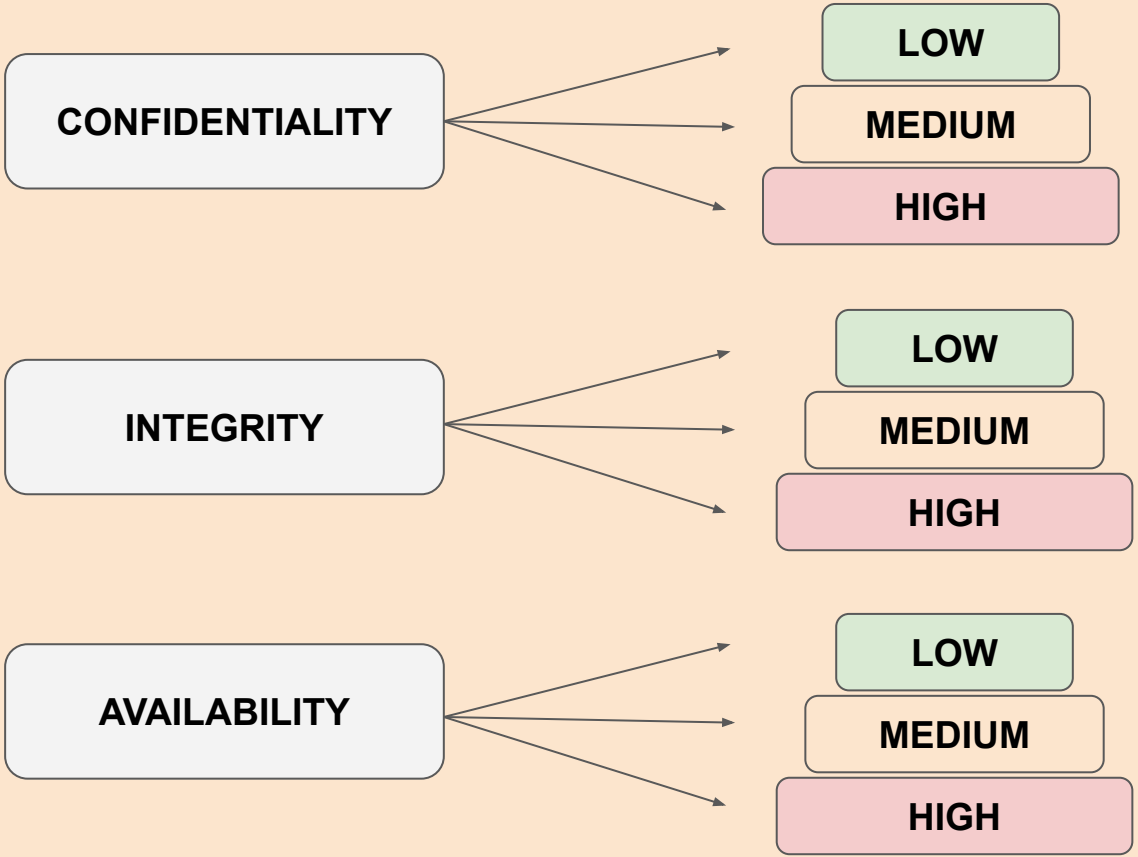
ADVERSARY OR ATTACKER	An entity that attacks, or is a threat to, a system.
HACKER	Black hat hacker: Who attempts to gain unauthorised access or entry into a system. White hat hacker: An individual who helps organisations to strengthen the security of a system.
ATTACK	An action that compromises security of the system. Inside Attack: Initiated by an entity (i.e., an insider) inside the security perimeter Outside Attack: Initiated from outside the perimeter (i.e., an outsider), by an unauthorised entity
COUNTERMEASURE	An action, procedure or technique that reduces a threat, a vulnerability, or an attack.
RISK	The probability that a threat will exploit a vulnerability with a particular harmful result.
SECURITY POLICY	A set of security rules and practice guidelines that specify or regulate how a system or organisation provides security services. The goal is to protect sensitive and critical system resources.
SYSTEM RESOURCE OR ASSET	Data contained in an information system, a service provided by a system, and system capability such as processing power or communication bandwidth.
THREAT	A potential for violation of security. Could breach security and cause harm. A possible danger that might exploit a vulnerability.
VULNERABILITY	A flaw or weakness in a system's design, implementation, or operation and management that could be exploited.

LOSS OF SECURITY

Loss of confidentiality: unauthorised disclosure of information
Loss of integrity: unauthorised modification or destruction of information
Loss of availability: disruption of access to or use of information or services

LEVELS OF IMPACT DUE TO LOSS OF SECURITY




CONFIDENTIALITY
LOW
MEDIUM
HIGH
INTEGRITY
LOW
MEDIUM
HIGH
AVAILABILITY
LOW
MEDIUM
HIGH

NETWORK SECURITY

"Network Security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorised access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment"

THE OSI* SECURITY ARCHITECTURE

The framework of protocols, standards, and mechanisms designed to ensure the security of data and communications within a network environment following the OSI model's layered approach.

SECURITY ATTACK	An action that compromises security of system or exchanged information
SECURITY SERVICE	A service that enhances security of system or exchanged information
SECURITY MECHANISM	A mechanism that is designed to detect, prevent, or recover from a security attack.

PASSIVE SECURITY ATTACK

Release of message content
An eavesdropper intercepts and reads sensitive email exchanges between executives of a company.

Traffic analysis
An attacker monitors the frequency and timing of messages between two parties to infer patterns and possibly the importance of the communication without reading the actual messages.

ACTIVE SECURITY ATTACK

Message modification
An attacker intercepts a message, alters its content, and sends it on to the intended recipient, causing misinformation or a change in the message's intended action.

Replay
An attacker intercepts a valid data transmission and retransmits it to create an unauthorised effect, such as reusing an authentication token to gain access.

Masquerade
An attacker pretends to be a legitimate user by using stolen credentials to access restricted areas of a network.

Denial of Service (DoS)
An attacker floods a server with excessive requests, overwhelming the system and preventing legitimate users from accessing the service.

SECURITY SERVICES

- A process of identifying and verifying whether the communicating entity is the one it claims to be. → **Authentication**
- A technique used to regulate access to resources → **Access Control**
- Protection of the data → **Confidentiality (Message)**
- Protection of the data → **Confidentiality (Header)**
- Ensuring received data is not tampered by unauthorised entities → **Data Integrity**
- Protection against denial by communicating entities → **Non-repudiation**
- The property of a system being accessible and usable upon demand → **Availability**

	Release of Message Content	Traffic Analysis	Masquerade	Replay	Message Modification	Denial of Service
Authentication						
Access Control						
Confidentiality (Message)						
Confidentiality (Header)						
Data Integrity						
Non-repudiation						
Availability						

SECURITY MECHANISMS

PASSWORD

A secret word or phrase known to an authorised party

DIGITAL SIGNATURE

A cryptographic technique that allows recipients to validate message authenticity

ENCRYPTION

encoding messages in such a way that only authorised parties can read it

NOTARIZATION

A document that has been signed by a notary public in order to make it official or legal

ACCESS CONTROL MECHANISM

Techniques for enforcing access rights

SECURITY SERVICES vs MECHANISMS

	ENCRYPTION	DIGITAL SIGNATURE	ACCESS CONTROL MECHANISM	NOTARISATION	PASSWORD
Authentication (A process of identifying and verifying whether the communicating entity is the one it claims to be.)					
Access Control (A technique used to regulate access to resources)					
Confidentiality (Message) (Protection of the data)					
Confidentiality (Header) (Protection of the data)					
Data Integrity (Ensuring received data is not tampered by unauthorised entities)					
Non-repudiation (Protection against denial by communicating entities)					
Availability (The property of a system being accessible and usable upon demand)					

COMPUTER SECURITY

"Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer"

NETWORK SECURITY

"Measures to protect the underlying networking infrastructure from unauthorised access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment”

CYBER SECURITY

"The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets"

CYBER SECURITY

Overlaps with information security

More specific to cyberspace

Incorporates the human factor
Relates to the role of human in the security process

Cyber security is not only about the CIA triad

Cyber crime/Cyber bullying/ Cyber terrorism

NZ's CYBER SECURITY STRATEGY

– Exercising cyber resilience

– Having cyber capabilities

– Improving cyber security

– Increasing international cooperation

GDPR

Data Protection Directive (DPD)
deals with the protection and processing of personal data EXCLUDING citizens outside of the EU

GDPR replaces DPD
GDPR legally protects personal data of EU citizens outside of the EU.

GDPR extends the definition of personal data to:

- Photos, audio, videos, financial transactions, social media posts, etc.
- Device identifiers (IP address, IMEI number)
- Browsing history
- Genetic information

TYPES OF DATA

PERSONAL DATA	Any information related to an identified or identifiable person. **EG** ID, gender, address
DE-IDENTIFIED DATA	Personal data without any personal identifiers **EG** anonymous post in FB group
ANONYMIZED DATA	Personal data without identifiers, where it is impossible to re-identify **EG** average age of first home buyers

TYPES OF SUBJECTS

DATA SUBJECT	any person whose personal data is being collected, held, or processed **EG** Students and Staff
DATA CONTROLLER	An entity that determines the purposes and means of personal data processing. **EG** UoA
DATA PROCESSOR	An entity that handles personal data on behalf of data controllers **EG** Google (Gmail)

GDPR PRINCIPLES

- Accuracy
  - states that data gathered from clients must be stored correctly and updated regularly
- Lawfulness, fairness, and transparency
  - states that the gathered data must be handled legitimately, impartially, and transparently
- Purpose limitations
  - states that clients' data must NOT be utilized in ways unknown to the client
- Data minimization
  - states that ONLY data directly relevant to a specified purpose should be collected
- Accuracy
  - states that data gathered from clients must be stored correctly and updated regularly

IN TERMS OF THE CIA TRIAD

- Confidentiality
  - confidentiality states that ONLY those with the requisite authorization are allowed to retrieve clients' data.
- Integrity
  - integrity, on the other hand, states that the retrieved client's data should ONLY be altered by those who have been authorized to carry out such alterations
- Accountability
  - accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles.

GDPR KEY CHANGES

1

INCREASED TERRITORIAL SCOPE (EXTRATERRITORIAL APPLICABILITY)

- GDPR applies to all companies processing the personal data of EU data subjects, data controllers and data processors.

2

PENALTIES

- Maximum Fine: up to 4% of annual global turnover or €20 million (whichever is greater)

3

CONSENT

- The request for consent must be given in an understandable and easily accessible form with the purpose stated.
- Consent must be clear and in plain language
- Consent is easily withdrawable.

Data Subject Rights

BREACH NOTIFICATION	Must be done within 72 hours after becoming aware of the breach.	Data controllers and data processors are required to notify their customers
RIGHT TO ACCESS	A confirmation from data controllers as to whether or not personal data concerning them is being processed, where and for what purpose	The controller shall provide a copy of personal data free of charge amd in electronic format
RIGHT TO BE FORGOTTEN	Also known as Data Erasure, entitling data subjects to have the data controller erase personal data.	Data controllers must check “the public interest in the availability of the data”
DATA PORTABILITY	Data subjects have the right to request and receive personal data that have been provided to data controller in a structured, readable format. Also, subjects can request data to transmit from one controller to another.	Data controllers should accept and send their data. This only applies to personal data and NOT anonymous data.
PRIVACY BY DESIGN	Inclusion of data protection from the early stages of the system design. The controller can hold and process only the data exactly necessary for the completion of its duties.	The controller shall implement “data protection through technology design”

PASSWORDS

IDENTIFICATION vs AUTHENTICATION

IDENTIFICATION

The process in which a system entity provides its claimed identity

EG: UPI (unique personal identifier)

AUTHENTICATION

The process of verifying an identity claimed by a system entity

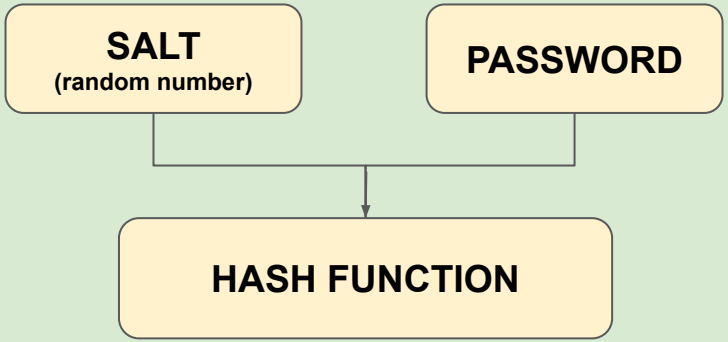
EG: PIN (personal identification number) or password

PASSWORD VULNERABILITIES

		COUNTER-MEASURES
Offline dictionary attack	Attackers gain access to password files (hash values of passwords) and compare these hashes against hashes of commonly used passwords.	Prevent access to hashed password files or rapid reissuance of passwords.
Specific account attack	Attackers target a specific account, submits password guesses until successful.	Lock out mechanism after certain number of attempts or delay subsequent tries.
Popular password attack	Attackers try commonly used passwords such as "QWERTY" or "1234" against a wide range of user ID's.	Enforce complex password policies, intrusion detection, or scanning IP's to submission patterns.
Password guessing (single user)	Gaining knowledge about an individual user and knowing system password policies together to guess a password.	Educate users and enforce complex password policies.
Workstation hijacking	The attacker waits until a logged-in workstation is unattended	Logging out after a certain period of inactivity or Intrusion detection schemes that detect changes in user behaviour
Exploiting user mistakes	Users writing their passwords down as they are hard to remember, where an attacker uses social engineering to trick user into revealing password.	Changing default passwords such as "Stationery" or to educate users.
Exploiting same password use	Attackers learn a password from one source, and this ends up being the same password for multiple services for one user.	Educate users to choose different passwords for all sites.
Electronic monitoring	Communicating a password in plaintext is vulnerable to eavesdropping	Never send a password in plaintext or Technical solutions for secure transfer of passwords

COUNTERMEASURES

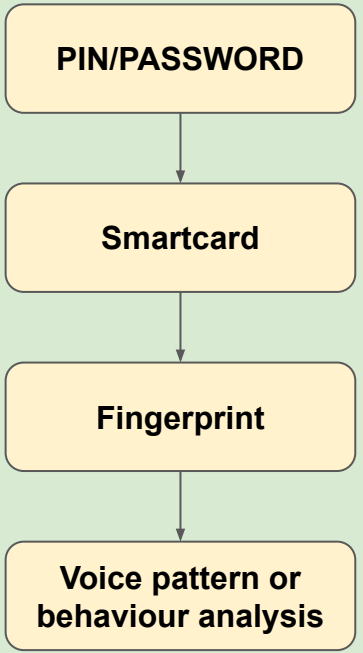
SALT WITH HASH



1. The user provides User ID and password
2. Lookup the corresponding salt and hash
3. Re-compute the hash based on the retrieved salt and entered password
4. If the result matches, password is accepted.

- Difficult to guess if one user chooses the same password for multiple services.
- Difficult to guess if multiple users choose the same password for a single service (or more)
- Makes offline dictionary attack difficult
- Protection against rainbow tables, pre-computed hash values (EG with every possible salt). The solution is to use a large salt.

MULTI-FACTOR AUTHENTICATION



MAN-IN-THE-MIDDLE ATTACK (MITM)

Requests to download file

Please insert email address

Sends email address

Security Question What is the name of your best friend?

Answer: Bob

I forgot my password.

Security Question What is the name of your best friend?

Answer: Bob

Choose new password

Google

COUNTERMEASURES:

- Educate users
- Use MFA (Multi-factor authentication
- Better notifications to users for password reset
- Phone call and reply by voice in case of password reset

ACCESS CONTROL

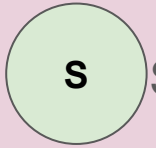
AUTHORISATION

A process of granting rights or permissions to a system entity to provide access to a given resource.

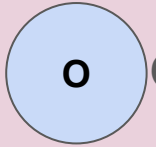
REQUIREMENTS

RELIABLE INPUTS	Authenticated entities. **EG** UPI and password
PRINCIPLE OF LEAST PRIVILEGE	Deals with granting the minimum set of access rights to do a job. **EG** accessing a single course vs all courses
ADMINISTRATIVE DUTIES	Only a special entity should be able to manage access rights. **EG** granting, revoking, or updating access rights

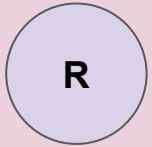
ELEMENTS TO ACCESS CONTROL



Subject: an entity that can access objects.



Object: An entity that needs to be protected.



Right: Describes how a subject can access and object.

function(s, o, r): looks up access right for combination (s,o). On successful match, it grants access, otherwise not.

Security Administrator: An entity that manages access rights.
Auditor: An entity that inspects the whole authorisation system.

ACCESS CONTROL MODELS

Discretionary Access Control (DAC)

- Resource owner decide who can access and level of access.
- Access is granted based on identity of the requester.
- Vulnerable to Trojan horses.
- DAC is used in operating systems (Linux file permissions: rwxr-x--x, read(r), write(w), execute(x))

	FILE1	FILE2	FILE3	FILE4
ALICE	Own Read Write		Own Read Write	
BOB	Read	Own Read Write	Write	Read
CHARLI	Read Write	Read		Own Read Write

Role-Based Access Control (RBAC)

- RBAC maps roles (e.g., in an organization) to access
- rights
- Supports complex access control
- Reduces errors in administration, compared to user- assigned access
- Ease of administration
  - Move users in and out of roles
  - Move permissions in and out of roles
  - Very flexible, compliance within organization
- Least privilege
  - Restricts access according to needs
  - Separation of duties through constraints

MALICIOUS SOFT**WARE**

MALWARE

Malware is a set of instructions (programs) that run on your computer aiming to compromise CIA.

MALWARE TYPES

VIRUS
An executable or script that replicates itself

WORM
A computer program that can run independently and propagate itself over the network

TROJAN HORSE
It appears to have a useful function, but also has a hidden and potentially malicious function

SPYWARE
Software that collects information from and transmits it to another system

RANSOMWARE
Stealing data and asking for money to get it back

BOTNETS
Receive commands from remote Command and Control (C&C) servers

COUNTERMEASURES

- FIREWALLS
- ANTI-VIRUS
- INTRUSION DETECTION SYSTEM (IDS)
- INTRUSION PREVENTION SYSTEM (IPS)
- MALWARE DETECTION
- PHISHING-DETECTION SYSTEMS
- EDUCATE USERS
- BLACKLISTING IPS
- PATCH YOUR MACHINE

EG: DOCUMENT BASED MALWARE

- The malware embeds malicious codes into documents, PDFs, spreadsheets, and other files
- Once on your computer, it can perform various malicious tasks such as stealing passwords or infecting your email contacts
- The worst part is that you can activate the malware through normal day-to-day tasks such as opening your emails.
- Document-based malware overrides your commands, altering your computer, causing damage and further spreading the malicious code

- Often, the malware tampers with word processors by adding, deleting, and changing words within your documents
- It moves text, adds images, and corrupts your hard drive.
- It can infiltrate your email, sending unsolicited emails to your contact list. Unsuspecting recipients will open your emails in good faith, spreading the virus into their computers.

EG: ADVANCED PERSISTENT THREAT (APT)

- Using a wide variety of intrusion technologies and malware while applying persistently and effectively to specific targets where it runs over an extended period.

EG: ZERO-DAY

- An unknown flaw that is discovered but does not have a patch or other fix (0-day to prepare a patch) where it can be exploited.

EG: BACKDOOR

- Any mechanism that bypasses a normal security check
- It may allow unauthorized access to data or program functionalities

EG: SOCIAL ENGINEERING

- Psychological manipulation to trick users into doing security mistakes or giving away sensitive information
- Phishing is the most popular type: Email and text message aimed at creating a sense of urgency, curiosity or fear in victims