=> Mid 1 :

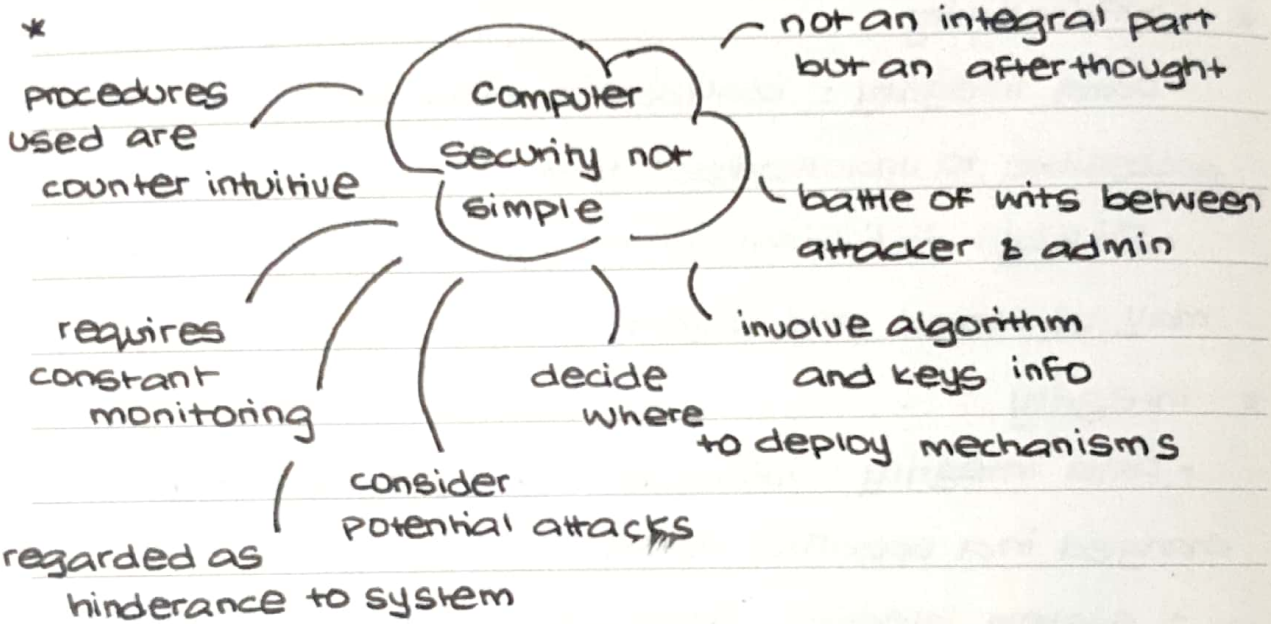
Chapter 1 - Principles and Practices

* computer security - protection provided to an information system to attain confidentiality, integrity and availability to its resources.
* confidentiality
  - Data integrity : confidential information not accessible to unauthorized user
  - Privacy : individual control on what information may be stored and collected
* integrity
  - Data integrity : information and program only changed in a specified manner
  - system integrity : system performs its operations in not damaged manner
* Availability - system works promptly and service not denied to users
* Authenticity - to be able to be genuie and be able to be verified and trusted, confidence in the validity
* Accountability - requirement for action to be traced uniquely to an individual to support non-repudation, deference and fault isolation

SANDEN
SANPAK ENGINEERING INDUSTRIES (PVT) LTD.

* Levels of impact - loss that has effect on organizational assets of, organizational operations or individuals
  - Low : expected to have limited effect
  - Moderate : expected to have serious adverse effect
  - High : expected to have serious or catastrophic effect

*



* Assests of a computer system are hardware, software, data and communication facilities and networks
* Adversary (threat agent) - anyone that conducts or intents to conduct detrimental activities
* Attack - malicious activity to collect, disrupt, deny, degrade, destroy information security resources or information
* Countermeasure - device/technique for impairment

of operational effectiveness of undesirable or adversarial activity.

* Risk - a measure to see extent an entity is threatened by occurence of an event. 1) adverse impacts arised when event occurs and 2) likelihood of occurence.

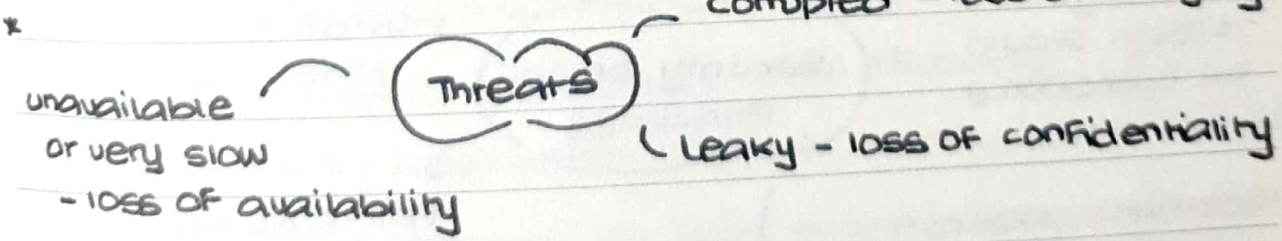
* security Policy - set of criteria defining the constrains and activities of data processing to maintain security for systems and data.

* System Resource (Asset) - major application, general support system, high impact program, personnel, equipment or logically related group of systems

* Threat - circumstance/event to adversary effect organization through unauthorized access, DOS, ~~des~~ destruction & or disclosure

* Vulnerability - weakness in an information system or implementation that could be exploited or triggered by a threat source.

*



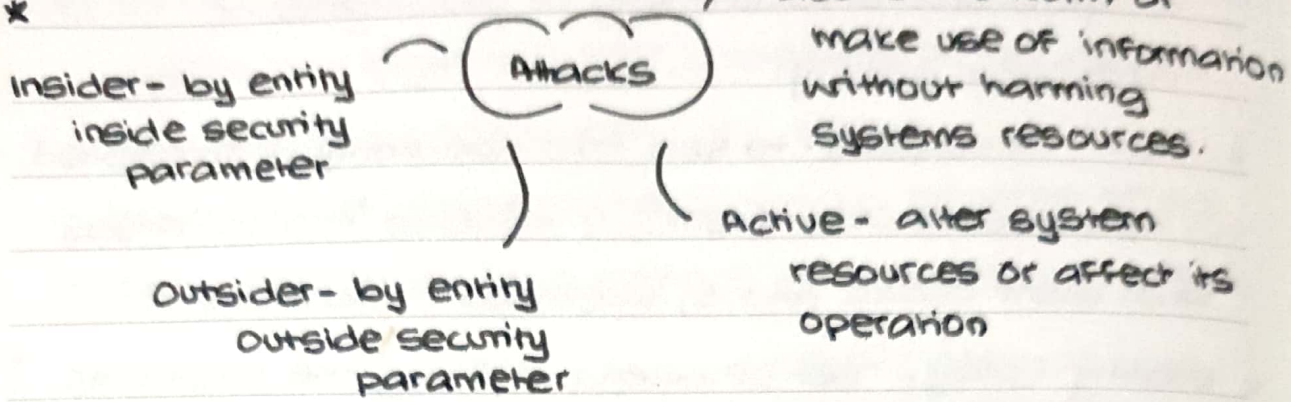
* Threats exploit vulnerabilities to potentially harm an asset

Date ____/____/____

MON TUE WED THU FRI SAT SUN

SANDEN
SANPAK ENGINEERING INDUSTRIES (PVT) LTD.

*

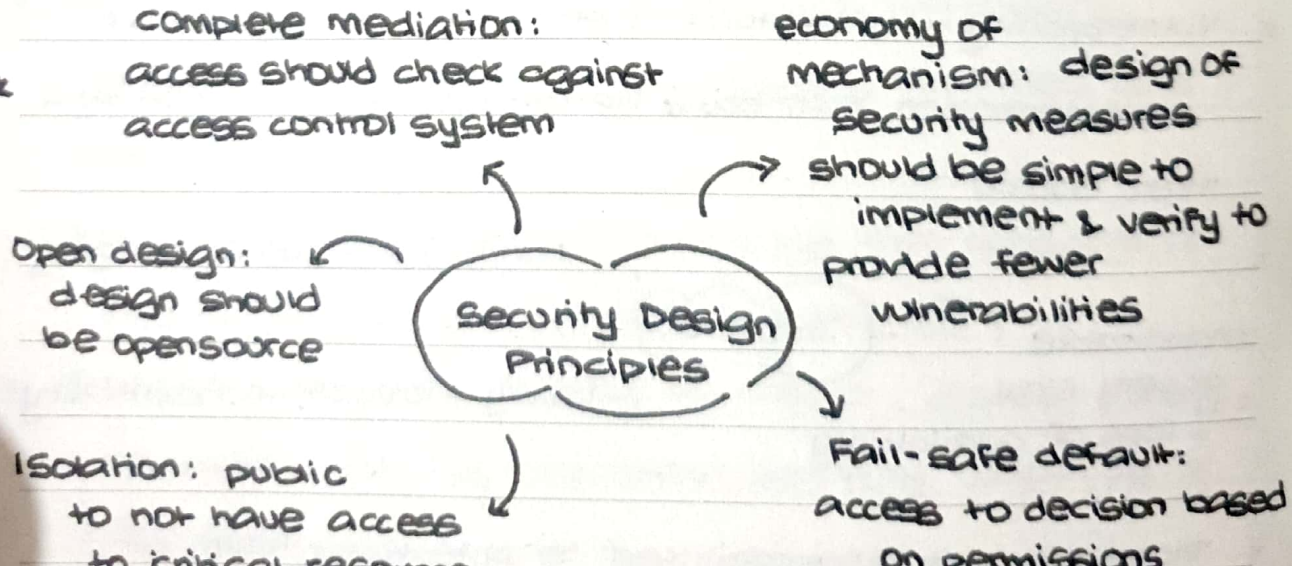


* Deal with security attacks by prevent, detect and recover.

* Scope of computer security:

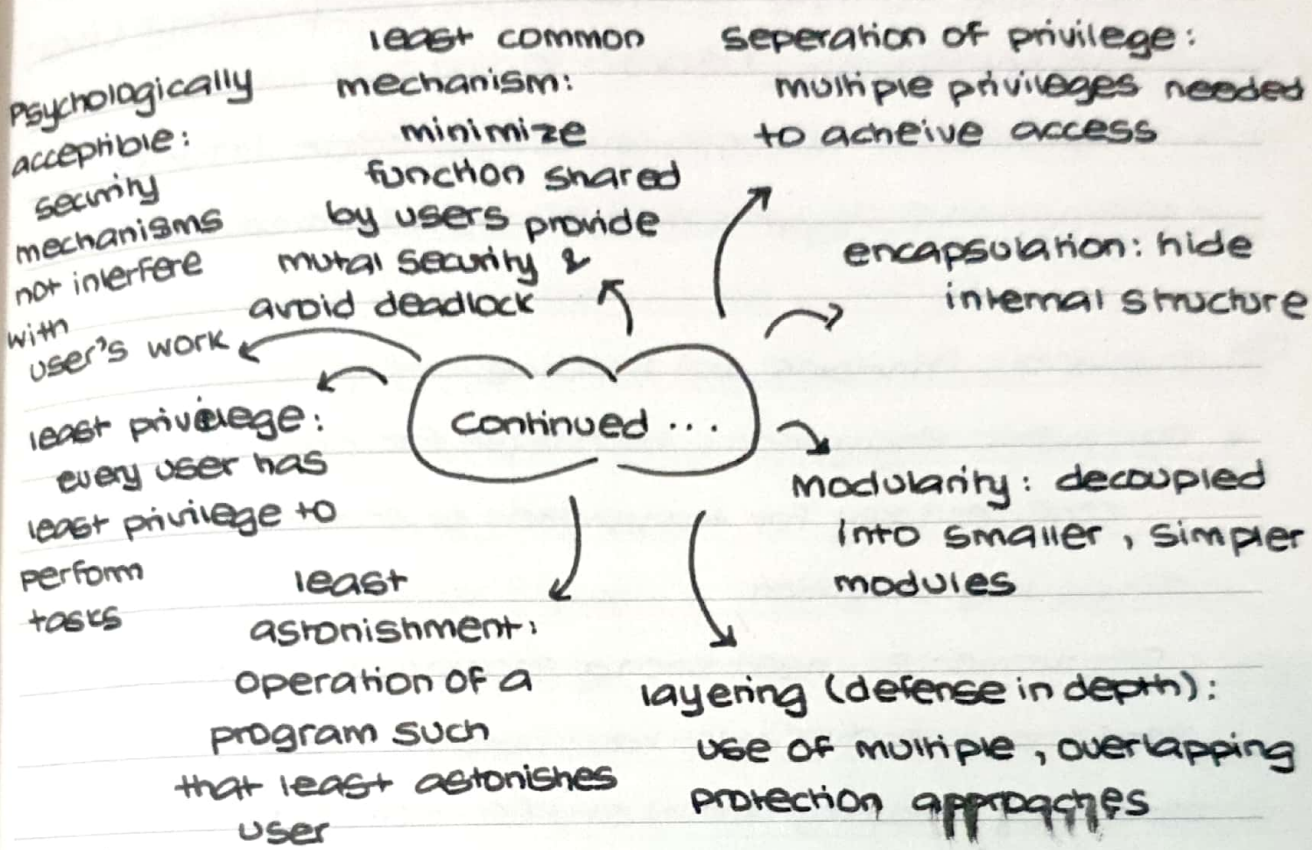
- Protection: access to data must be controlled.
- User authentication: access to computer facility controlled.
- Network Security: data transmitted securely through networks.
- File security: sensitive files must be secure

*



www.sanpak.biz

SANDEN
SANPAK ENGINEERING INDUSTRIES (PVT) LTD.



* Overall strategy for providing security:
  - Policy: what security schemes are supposed to do assets & their values, potential threats, ease of use vs security, cost of security vs cost of failure.
  - Implementation / mechanism: how to enforce prevention, detection, response and recovery
  - Correctness / assurance: does it work, validation / review
* Standards - developed to cover managment practices and overall architecture of security mechanisms and services.

Date ____ / ____ / ____

MON TUE WED THU FRI SAT SUN

SANDEN
SANPAK ENGINEERING INDUSTRIES (PVT) LTD.

- National institute of Standards & Technology (NIST)
- Internet Society (ISOC)
- International Telecommunication Union (ITU-T)
- International Organization of Standardization (ISO)