

## es Mid 1:

The Chapter 1 - Principles and Practices

- 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
- 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

www.sanpak.biz



- \* Levels of Impact 1055 that has effect on 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

not an integral part K but an afterthought procedures computer used are Security not counter intuitive - battle of wits between SIMPLE attacker & admin involve algorithm requires and keys info decide constant monitoring Where to deploy mechanisms consider potential attacks regarded as hinderance to system

- \* 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 impaiment

www.sanpak.biz





of operational effectiveness of undesirable or adversarial activity.

- k 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.
- and activities of data processing to maintain security for systems and data.
- general support system, high impact program, personnel, equipment or logically related group of systems
- \* Threat circumstance/event to adversary effect organization through unauthorized access, oos, des destruction a or disclosure
- \* Vulnerability weakness in an information system or implementation that could be exploited or triggered by a threat source.

unavailable Threats compled - 1066 of integrity
or very slow
- 1066 of availability

t Threats exploit vulnerabilities to potentially harm an

Date		1				
MON	TUE	WED	THU	FRI	SAT	SUN



insider- by entity inside security parameter Attacks

Passive - to learn or make use of information without harming systems resources.

outsider - by entity
outside security
parameter

resources or affect its operation

- \* 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 contoned
  - Network Security: data transmitted Securely through networks .
    - File security : sensitive files must be secure

access control system

economy of
mechanism: design of
security measures
should be simple to
implement & verify to
provide fewer

vulnerabilities

open design: k design should be opensource

Security Design

to not have access to critical resource,

Fair-safe default: access to decision based on permissions

security measures
isolated from one another,
www.sanpak.biz

prevent access to them.





provection approaches

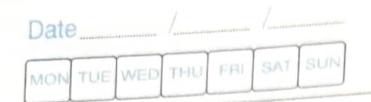
seperation of privilege: least common Psychologically multiple privileges needed mechanism: acceptible: to acheive access minimize function shared security mechanisms by users provide encapsulation: hide not interfere mutal security & internal structure avoid deadlock with user's work least privalege: continued .. every user has modularity: decoupled least privilege to into smaller, simpler perform least modules tosks astonishment layering (defense in depth): operation of a program such use of multiple, overlapping

\* overall strategy for providing security:

that least astonishes

user

- Policy: what security schemes are supposed to do assets & their values, potential threats, ease of use VS security, cost of security us cost of failure.
- Implementation / mechanism: how to enforce prevention, detection, response and recovery
- correctness | assurance: does it work, validation | review k standards developed to cover managment practices and overall architecture of security mechanisms and services.





- National institute of Standards & Technology (NIST)
- Internet Society (150c)
- International Telecommunication Union (170-7)
- International Organization of Standardization (130)