Threat Consequence and Threat Action (Attack)

* Unauthorized Disclosure – A circumstance or event whereby an entity gains access to data for which the entity is not authorized.
  + Exposure: Sensitive data are directly released to an unauthorized entity.
  + Interception: An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations.
  + Inference: A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications.
  + Intrusion.

Computer System

* Access to the data must be controlled (protection)
* Access to the computer facility must be controlled (user authentication)
* Data must be securely transmitted through networks (network security)
* Sensitive files must be secure (file security).
* Data processes representing users.
* Users making requests.

Computer and Network Assets, with Examples of Threats

* Hardware
  + Availability
    - Equipment Is stolen or disabled, thus denying service.
  + Confidentiality
    - An unencrypted CD-ROM or DVD is stolen
* Software
  + Availability
    - Programs are deleted denying access to users.
  + Confidentiality
    - An unauthorized copy of software is made.
  + Integrity
    - A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
* Data
  + Availability
    - Files are deleted, denying access to users.
  + Confidentiality
    - An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.
  + Integrity
    - Existing files are modified or new files are fabricated.
* Communication Lines and Networks
  + Availability
    - Messages are des

Passive and Active Attacks

* Passive Attack
  + Attempts to learn or make use of information from the system but does not affect system resources.
  + Eavesdropping on, or monitoring of, transmissions.
  + Goal of attacker is to obtain information that is being transmitted.
  + Two types:
    - Release of message contents
    - Traffic analysis
* Active Attack
  + Attempts to alter system resources or affect their operation.
  + Involve some modification of the data stream or the creation of a false stream.

Security Requirements

* Access control: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.
* Awareness and training: (i) Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, regulation, and policies related to the security risks associated with their activities and of the applicable laws, regulation, and policies related to the security of organizational information systems; and (ii) ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
* Media protection: (i) Protect information system media, both paper and digital

Design Principles

* Fundamental security design principles [1/4]
  + Despite years of research, it is still difficult to design systems that comprehensively prevent security flaws.
  + But good practices for good design have been documented (analogous to software engineering)
    - Economy of mechanism, fail-safe defaults, complete mediation, open design, separation of privileges, lease privilege, least common mechanism, psychological accountability, isolation, encapsulation, modularity, layering, least astonishment.
* Fundamental security design principles [2/4]
  + Economy of mechanism: the design of security measures should be as simple as possible
    - Simpler to implement and to verify
    - Fewer vulnerabilities
  + Fail-safe default: access decisions should be based on permissions; i.e., the default is lack of access
  + Complete mediation: every access should checked against an access control system.
  + Open design: the design should be open rather than secret (e.g., encryption algorithms)
* Fundamental security design principles [3/4]
  + Isolation
    - Public access should be isolated from critical resources (no connection between public and critical information)
    - Users files should be isolated from one another (except when desires)
    - Security mechanism should be isolated (i.e., preventing access to those mechanism)
  + Encapsulation: Similar to object concepts (hide internal structures)
  + Modularity: modular structure.
* Fundamental security design principles [4/4]
  + Layering (defense in depth): use of multiple, overlapping protection approaches
  + Least astonishment.
* Fundamental security design principles
  + Separation of privilege: multiple privileges should be needed to do achieve.
* Attack Surfaces
  + Attack surface: the reachable and exploitable vulnerabilities in a system.
    - Open ports
    - Services outside a firewall
    - An employee with access to sensitive info
    - …
  + Three categories
    - Network attack surface (i.e., network vulnerability)
    - Software attack surface (I.e., software vulnerabilities)
    - Human attack surface (e.g., social engineering)
  + Attack analysis: assessing the scale and severity of threats
* Attack trees
  + A branching, hierarchical data structure that represents a set
* An attack tree
  + Bank account compromise
    - User credential compromise
      * UT/Ula User surveillance
      * UT/Ulb /Theft of token and handwritten notes.
* Computer Security Strategy
  + An overall strategy for providing security
    - Policy (specs): what security schemes are supposed to do
      * Assets and their values
      * Potential threats
      * Ease of use vs security
      * Cost of security vs cost of failure/recovery
    - Implementation/mechanism: how to enforce
      * Prevention
      * Detection
      * Response
      * Recovery
    - Correctness/Assurance: does it really work (validation/review)
* Security Taxonomy
* Security Trends

Cryptographic Tools

* Symmetric Encryption
  + The universal technique for providing confidentiality for transmitted or stored data.
  + Also referred to as conventional encryption or single-key encryption.
  + Two requirements for secure use:
    - Need a strong encryption algorithm
    - Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.