Definitions and Terminology

Security Goals

- **Confidentiality**: concealment of information or resources.
- **Availability**: preserve ability to use information or resource desired.
  - An unavailable system is at least as bad as no system at all!

Security Goals (cont.)

- **Integrity**: trustworthiness of data or resources.
  - Typically refers to preventing improper or unauthorized modification
  - Data integrity (content of information)
  - Origin integrity (origin of information). Typically referred to as *authentication*.
    - E.g., user authentication refers to proving user is who they claim they are

Confidentiality

- Supported by access control methods
  - Cryptography for example
  - System-dependent mechanisms
    - BUT: These leave data public when they fail or are bypassed
- Also applies to existence of data
  - Knowing data exists can often be as valuable as the data itself

Confidentiality

- All confidentiality enforcement mechanisms require supporting services from system.
  - Assumption is that security services can rely on kernel and other agents, to supply correct data. Thus *assumptions* and *trust* underlie confidentiality mechanisms.
- **Confidentiality is not integrity**: just because no one can read it, doesn't mean they can't change it (and vice-versa)!

Integrity

- Example: the correct quote credited to the wrong source preserves data integrity but not origin integrity.

Integrity

- Affected by
  - Origin of data (how and from whom it was obtained)
  - How well data protected before arrival at current machine
  - How well data is protected on current machine
- Evaluating is difficult: relies on assumptions about source and about trust in that source

Availability

- Relevant to security because someone may be attempting to affect data or service by making it unavailable
  - Ex. Some software (e.g. network code) depends for correct operation on underlying statistical information and assumptions. By changing, for example, service request patterns, an adversary can cause this code to fail.

Availability

- Attack on availability is called a *denial of service* attack
  - Difficult to detect: is it a deliberate phenomenon or just an unusual access pattern? Also, even if underlying statistical model is accurate, atypical events do occur that may appear to be malicious!

Threat Related Terminology

- Vulnerability: Weakness (in security system) that might be exploited to cause loss or harm.

Threat Related Terminology

- Attack: actions that could cause violation to occur
- Attacker: those who cause such actions to be executed
- Passive attack: attacker merely observes (e.g., traffic analysis)
- Active attack: attacker actively modifies data or creates false data stream

Examples and Terms

- Snooping: unauthorized interception of information (form of disclosure). Countered by confidentiality mechanisms
  - Ex. Wiretapping

Examples and Terms

- Modification or alteration: unauthorized change of information
  - Ex. Active wiretapping
  - Ex. Person-in-the-middle attack: attacker reads message from sender and forwards (possibly modified) message to receiver. Countered by integrity mechanisms

Policy and Mechanism

- Security Policy: a statement of what is, and what is not, allowed
  - Setting policy can be tedious, but without policy, how do you know what is not allowed, let alone how to try to detect or prevent it?
- Security Mechanism: a method, tool, or procedure for enforcing a security policy
  - Mechanisms can be non-technical. Policies often require some procedural mechanisms that technology cannot enforce.

Policies and Mechanisms

- Policies may be presented mathematically, as a list of allowed and disallowed states.
  - In general an axiomatic description of secure states and insecure states
- In practice, rarely this precise
  - Normally written in English, leading to ambiguity (is a state legal or not?)

Assumptions and Trust

- Security rests on assumptions specific to the type of security required and the environment in which it is to be employed.
  - Ex. (Bishop) Opening a door lock requires a key. Assumption is that the lock is secure against lock picking. This assumption is treated as an axiom and made because most people require a key to open a locked door. A good lock picker can, however, open a locked door without a key. Thus in an environment with a skilled, untrustworthy lock picker, the assumption is wrong (and conclusions based on assumption may be invalid).

Assumptions and Trust

- Well-defined exception to rules provides a *back door* through which security mechanisms can be bypassed.
  - Trust resides in belief that back door will not be used except as specified by policy.

Assumptions and Trust

- Two assumptions made by policy designers
  - Policy correctly and unambiguously partitions set of system states into secure and insecure states
  - Security mechanisms prevent system from entering an insecure state
  - If either of these fail, system is not secure

Our First Security Principles

- Principle of Adequate Protection:
  - Computer systems must be protected to a degree consistent with their value
- Principle of Easiest Penetration:
  - Count on an intruder to use the easiest means to penetrate the system
  - I.e., System is most vulnerable at its weakest point (regardless of how well other points are defended).