CGS 3763: Operating System Concepts
Spring 2006

Security – Part 1

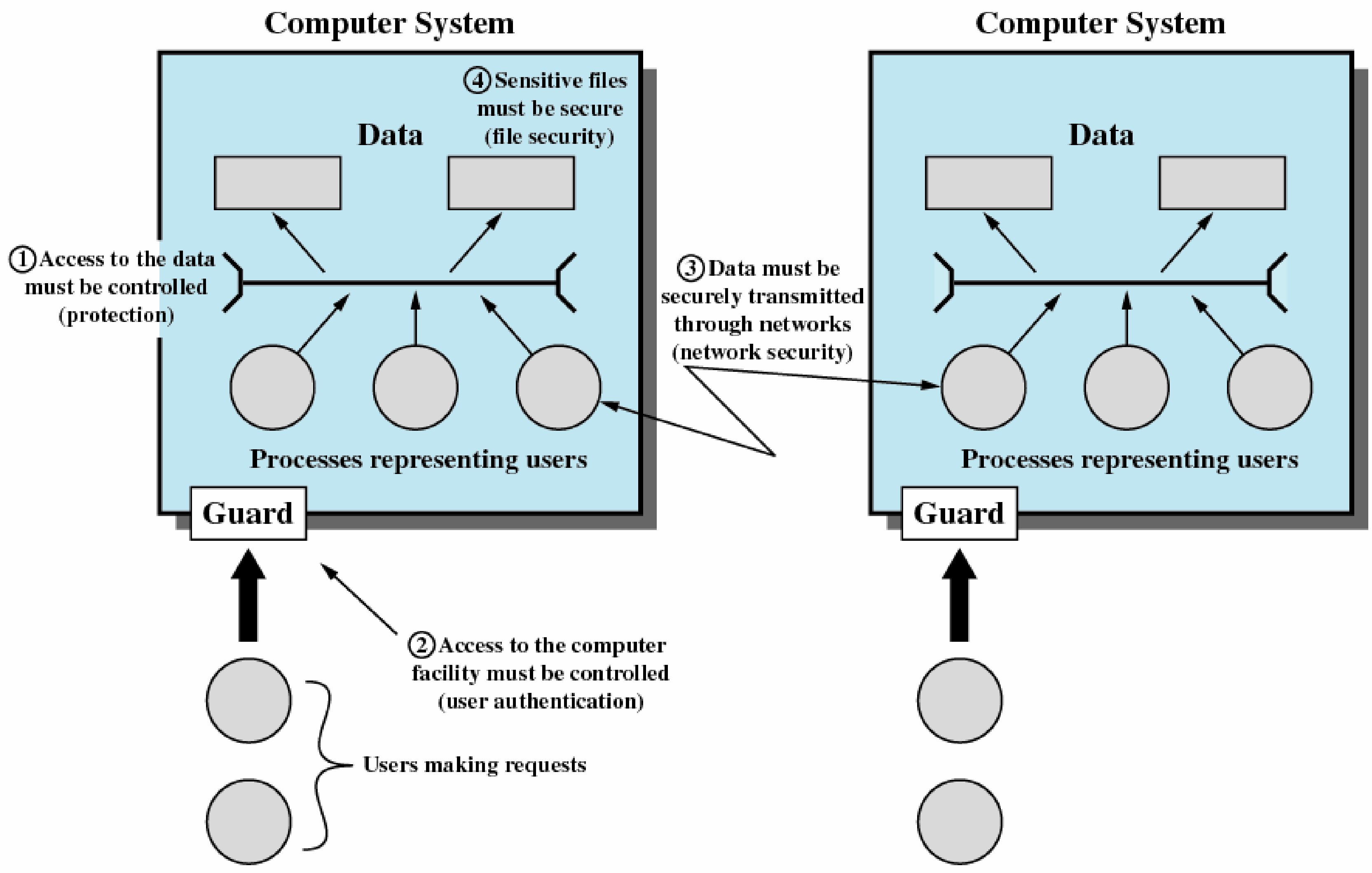
Instructor : Mark Llewellyn
markl@cs.ucf.edu
CSB 242, 823-2790
http://www.cs.ucf.edu/courses/cgs3763/spr2006

School of Electrical Engineering and Computer Science
University of Central Florida

The Security Problem

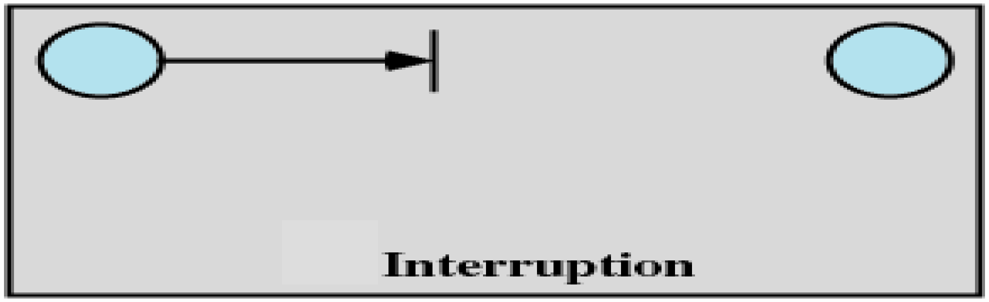
- Protection, as we discussed in the last section of notes, is strictly an internal problem: how to control access to programs and data stored in a computer system?
- Security, on the other hand, requires not only an adequate protection system but also consideration of the external environment in which the computer system operates.
  - A protection system is ineffective if user authentication is compromised or a program is run by an unauthorized user.
- Computer systems must be guarded against unauthorized access, malicious destruction or alteration, and accidental introduction of inconsistency.
  - Intruders (crackers) attempt to breach security.
- A threat is a potential security violation. An attack is attempt to breach security. Attacks can be accidental or malicious.
  - It is easier to protect against accidental misuse than malicious misuse.

The Security Problem (cont.)


Computer System
Computer System
Data
Data
④ Sensitive files must be secure (file security)
① Access to the data must be controlled (protection)
③ Data must be securely transmitted through networks (network security)
Processes representing users
Processes representing users
Guard
Guard
② Access to the computer facility must be controlled (user authentication)
Users making requests

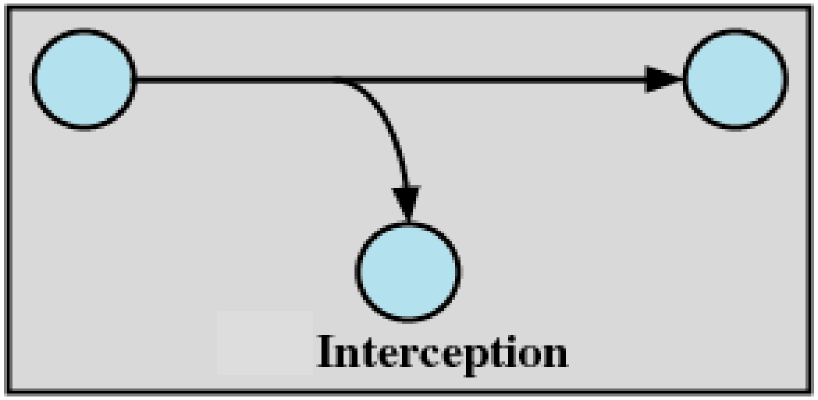
Types of Threats - Interruption

- Interruption
  - An asset of the system is destroyed or becomes unavailable or unusable
  - Attack on availability
  - Destruction of hardware
  - Cutting of a communication line
  - Disabling the file management system



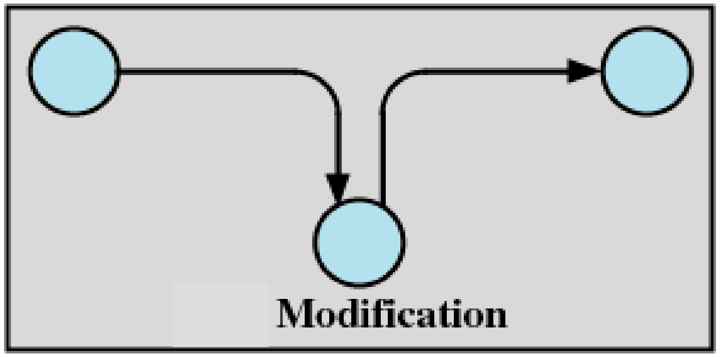
Types of Threats - Interception

- Interception
  - An unauthorized party gains access to an asset
  - Attack on confidentiality
  - Wiretapping to capture data in a network
  - Illicit copying of files or programs



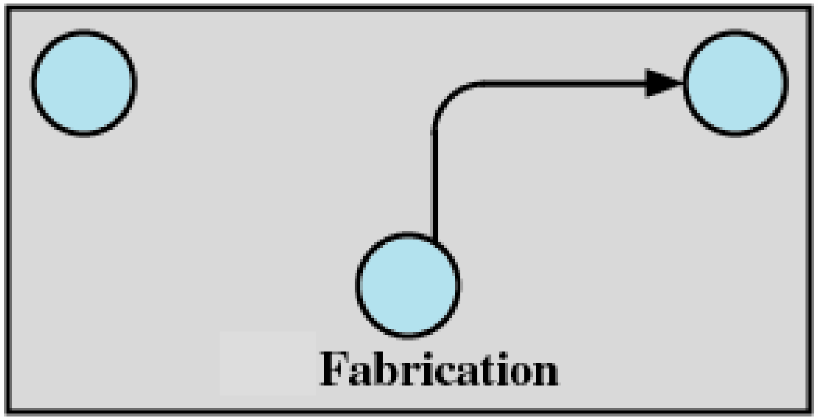
Types of Threats - Modification

- Modification
  - An unauthorized party not only gains access but tampers with an asset
  - Attack on integrity
  - Changing values in a data file
  - Altering a program so that it performs differently
  - Modifying the content of messages being transmitted in a network



Types of Threats - Fabrication

- Fabrication
  - An unauthorized party inserts counterfeit objects into the system
  - Attack on authenticity
  - Insertion of spurious messages in a network
  - Addition of records to a file



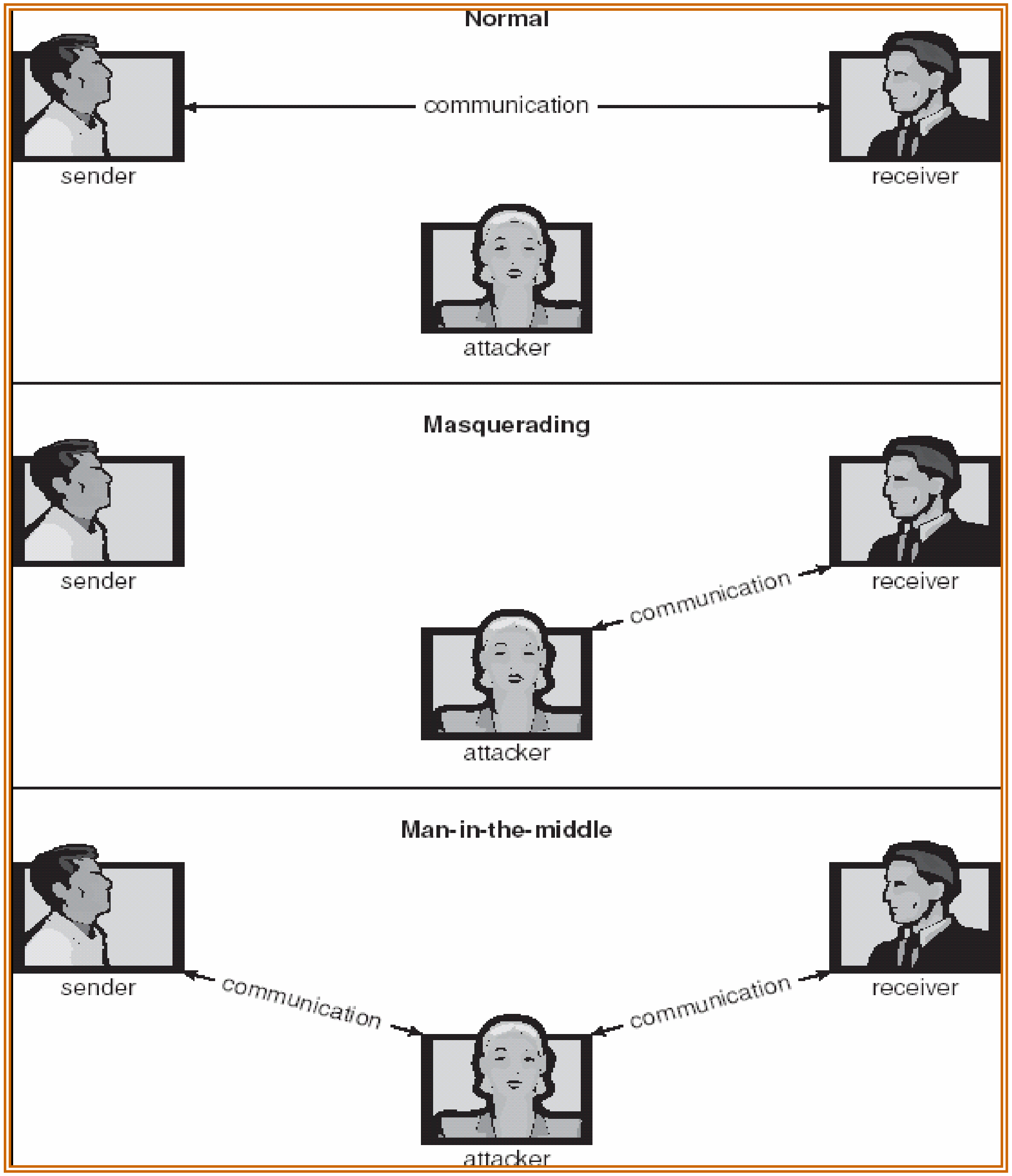
Categories of Attacks

- Breach of confidentiality – involves the unauthorized reading of data (or theft of information). Typically, a breach of confidentiality is the goal of an intruder, i.e., credit-card information theft.
- Breach of integrity – involves the unauthorized modification of data. Such attacks can result in passing of liability to an innocent party or modification of the source code of an important commercial application.
- Breach of availability – involves the authorized destruction of data. Some attackers (crackers) would rather wreak havoc and gain status or bragging rights than gain financially. Common in web-site defacement attacks.
- Theft of service – involves the unauthorized use of resources. For example, an intruder (or intrusion program) may install a daemon on a system that acts like a file server.
- Denial of service (DOS) – involves preventing legitimate use of the system. DOS attacks are sometimes accidental. The original Internet worm turned into a DOS attack when a bug in the code failed to delay its rapid spread.

Methods of Attack

- Masquerading (breach authentication) – one participant in a communication pretends to be someone else (another host or another person).
- Replay attack – consists of the malicious or fraudulent repeat of a valid data transmission.
  - Sometimes the replay compromises the entire attach, i.e., the repeat of a request to transfer money. But frequently it is done along with message modification, to escalate privileges, e.g., repeat request to transfer money but now into the unauthorized user's account!
- Man-in-the-middle attack – the attacker sits in the data flow of a communication, masquerading as the sender to the receiver, and vice versa. In a network communication, a man-in-the-middle attach is often preceded by session hijacking in which an active communication session is intercepted.

Standard Security Attacks



Security Measure Levels

- Security must occur at four levels to be effective:
  - Physical
  - Human
    - Avoid social engineering:
      - Phishing: A legitimate looking email or web page that misleads a user into entering confidential information.
      - Dumpster diving: A general term for attempting to gather information in order to gain unauthorized access to a computer by looking through trash, finding phone books, or notes containing passwords.
  - Operating System
  - Network
- Security is as weak as the weakest link in the chain.

Intrusion Techniques

- Objective of intruder is the gain access to the system or to increase the range of privileges accessible on a system.
- Often the protected information that an intruder acquires is a password.
- Password files can be protected in one of two ways:
  - One-way encryption – the system stores only the encrypted form of the user's password.
  - Access control – access to the password file is limited to one or a very few accounts.

Techniques for Learning Passwords

- Try default password used with standard accounts shipped with system
- Exhaustively try all short passwords
- Try words in dictionary or a list of likely passwords
- Collect information about users and use these items as passwords, e.g., names of children, birthdates, room numbers, etc.
- Try all legitimate license plate numbers for this state
- Use a Trojan horse to bypass restrictions on access
- Tap the line between a remote user and the host system

ID Provides Security

- Determines whether the user is authorized to gain access to a system
- Determines the privileges accorded to the user
  - – Superuser enables file access protected by the operating system
  - – Guest or anonymous accounts have more limited privileges than others
- ID is used for discretionary access control
  - – A user may grant permission to files to others by ID

Password Selection Strategies

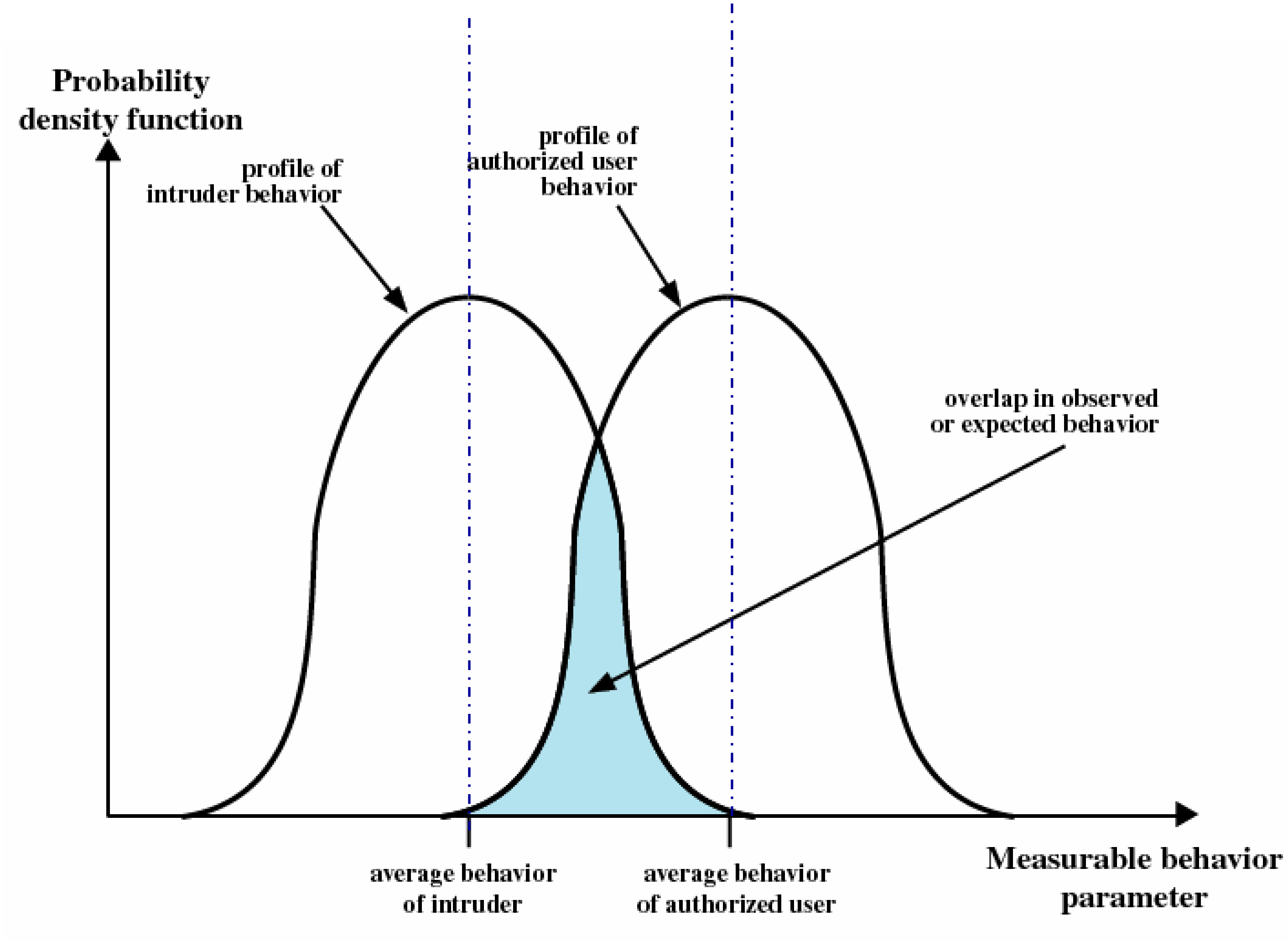
- User generated passwords
  - Users often choose absurdly short passwords which are easy to “guess”.
  - A Purdue University study examined approximately 7000 user accounts on 54 different machines and determined that 3% of the passwords were 3 characters or less in length.
  - Users often choose easily guessed passwords.
  - Another study examined 14,000 encrypted Unix passwords with a “guessing” program and was able to correctly determine 25% of the passwords.
- Computer generated passwords
  - Users have difficulty remembering them
  - Need to write it down
  - Have history of poor acceptance

Password Selection Strategies

- Reactive password checking strategy
  - System periodically runs its own password cracker to find guessable passwords
  - System cancels passwords that are guessed and notifies user
  - Consumes resources to do this
  - Hacker can use this on their own machine with a copy of the password file
- Proactive password checker
  - The system checks at the time of selection if the password is allowable
  - With guidance from the system users can select memorable passwords that are difficult to guess

Intrusion Detection

- Inevitably, the best intrusion prevention system will fail.
- A system’s second line of defense is intrusion detection and has been the focus of much attention in recent years.
- This interest is motivated by a number of considerations, including the following:
  1. If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data compromised.
  2. An effective intrusion detection system can serve as a deterrent acting to prevent intrusions.
  3. Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facilities.
- Intrusion detection is based on the assumption that the behavior of the intruder differs from that of a legitimate user.



Profiles of Behavior of Intruders and Authorized Users

Intrusion Detection Techniques

- Statistical anomaly detection
  - Collect data related to the behavior of legitimate users over a period of time.
  - Statistical tests are used to determine if the observed behavior is not legitimate behavior.
  - Confidence levels are set.
  - Threshold detection: thresholds are defined, independent of the user, for the frequency of various events.
  - Profile based: a profile of the activity of each user is developed an used to detect changes in the behavior of individual accounts.

Intrusion Detection Techniques

- Rule-based detection
  - Anomaly detection: rules are developed to detect deviation from previous usage pattern.
  - Penetration: identification: an expert system searches for suspicious behavior.

- To summarize: statistical-based approaches attempt to define normal, or expected behavior, whereas rule-based approaches attempt to define proper behavior.

Intrusion Detection (cont.)

- A fundamental tool for intrusion detection is the audit record. Some record of ongoing user activity must be maintained for input into an intrusion detection system.
  - Native audit records
    - All operating systems include accounting software that collects information on user activity
  - Detection-specific audit records
    - Collection facility can be implemented that generates audit records containing only that information required by the intrusion detection system