COP 4600 – Summer 2011

Introduction To Operating Systems

Security

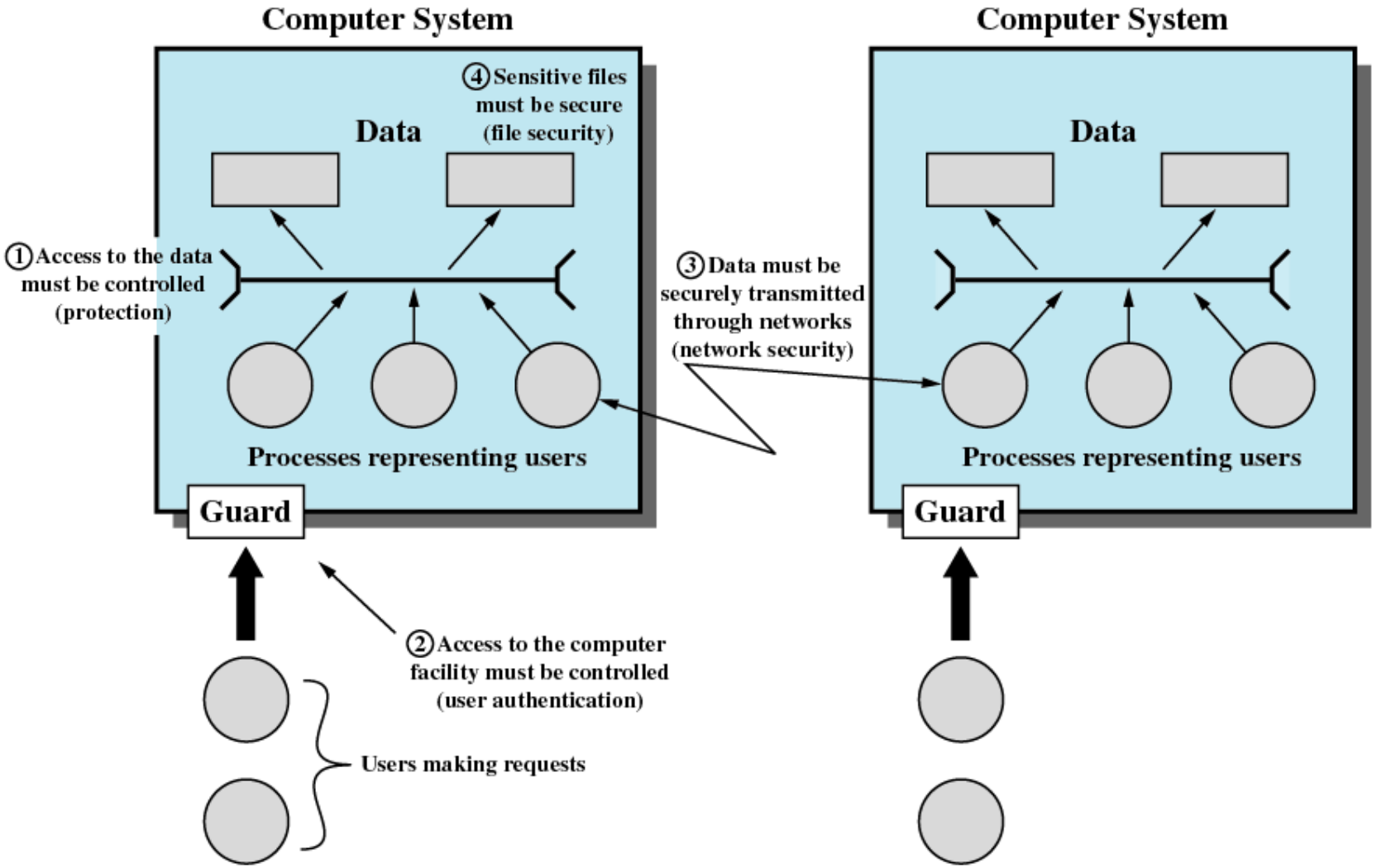
Instructor : Dr. Mark Llewellyn
markl@cs.ucf.edu
HEC 236, 407-823-2790
http://www.cs.ucf.edu/courses/cop4600/sum2011

Department of Electrical Engineering and Computer Science
Computer Science Division
University of Central Florida

The Security Problem

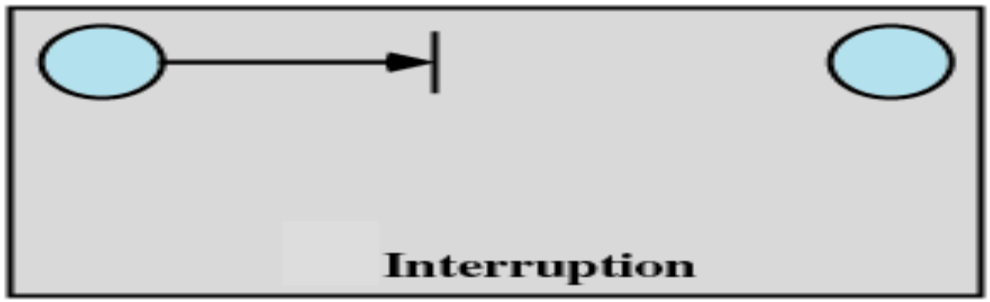
- Protection is strictly an internal problem: how to control access to programs and data stored in a computer system.
- Security, on the other hand, requires not only an adequate protection system but also consideration of the external environment in which the computer system operates.
  - A protection 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.)



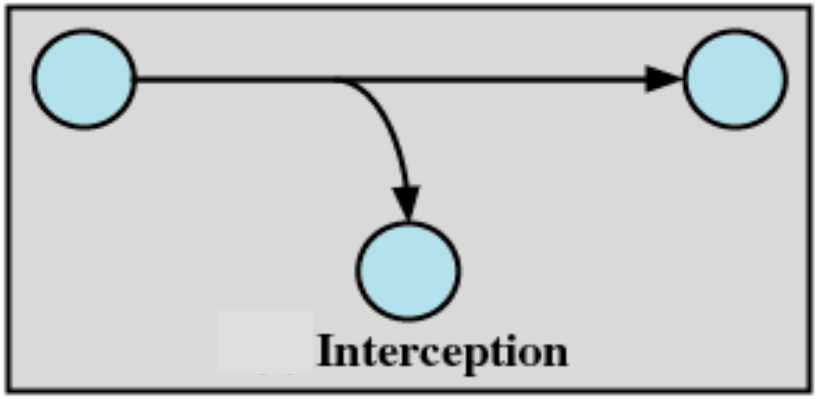
Types of Threats - Interruption

- 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



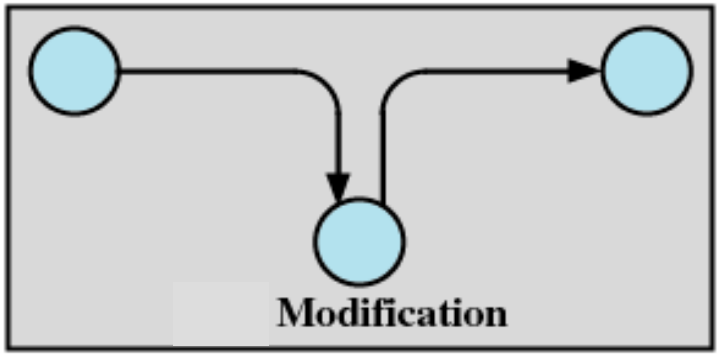
Types of Threats - Interception

- 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



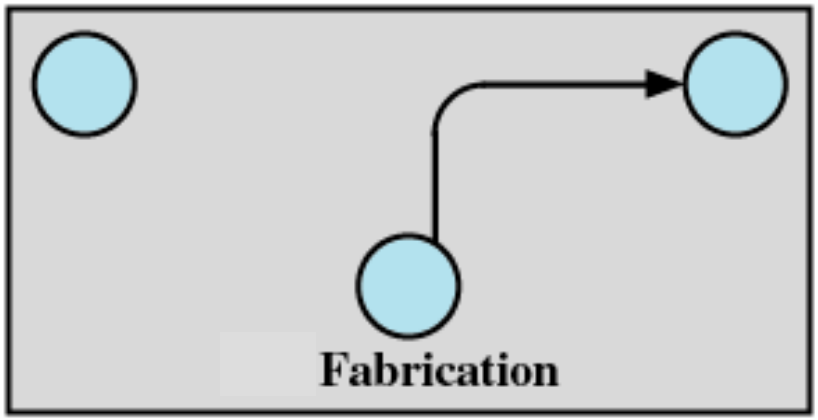
Types of Threats - Modification

- 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



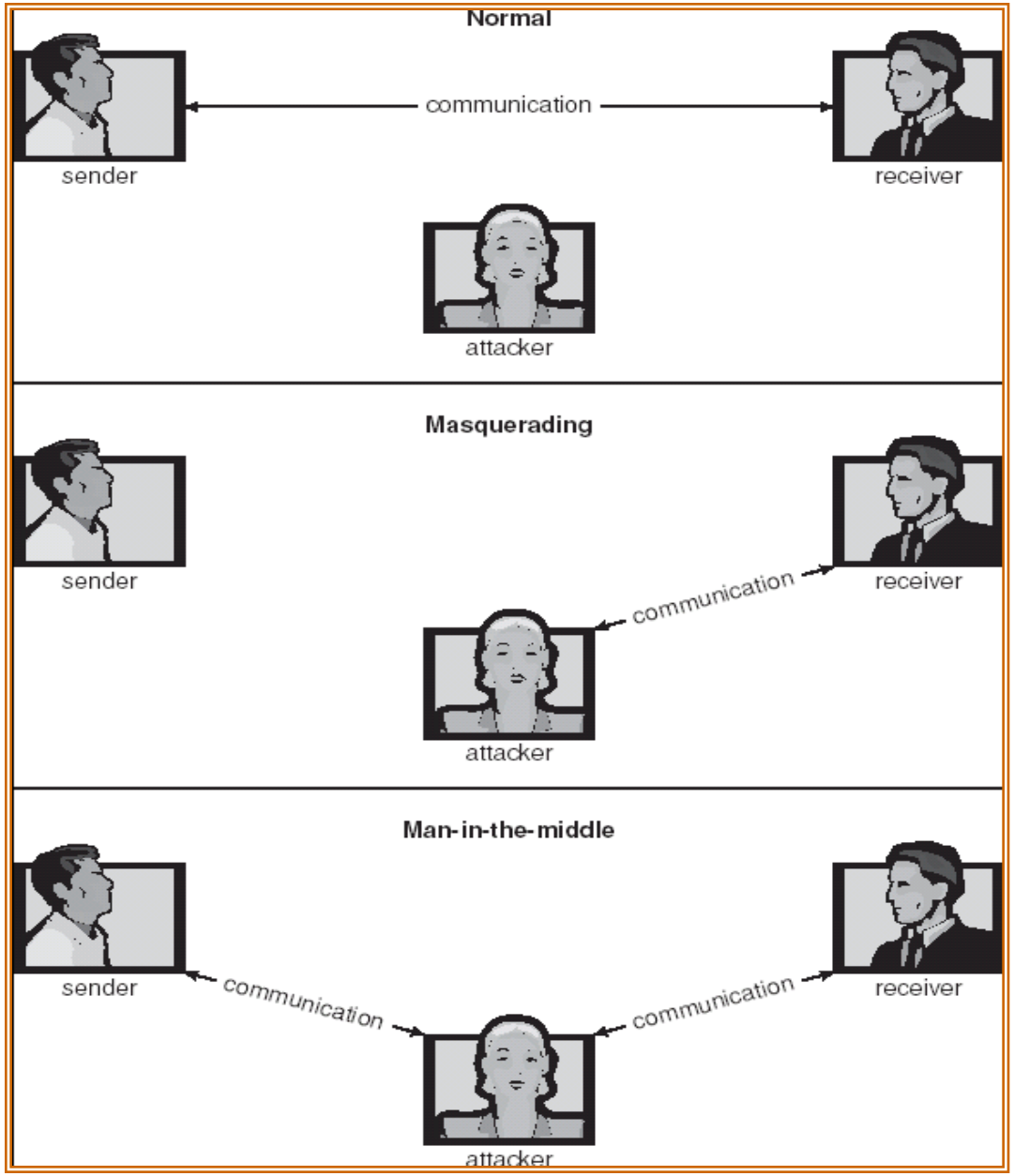
Categories of Attacks

- 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 attack, 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

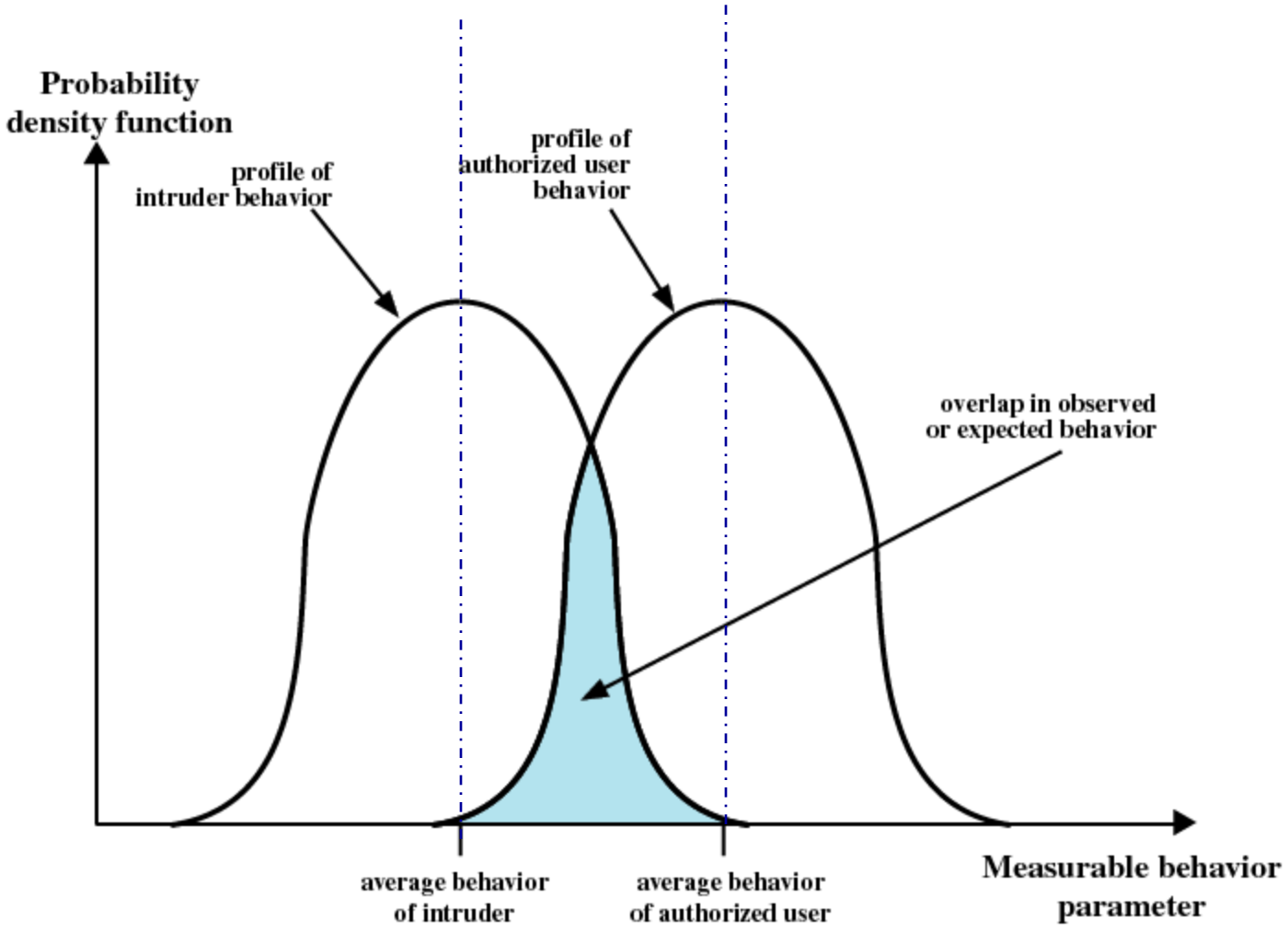
- User generated passwords
  - Users often choose absurdly short passwords which are easy to "guess".
  - A Purdue University study examined approximately 7000 user accounts on 54 different machines and determined that 3% of the passwords were 3 characters or less in length.
  - Users often choose easily 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.

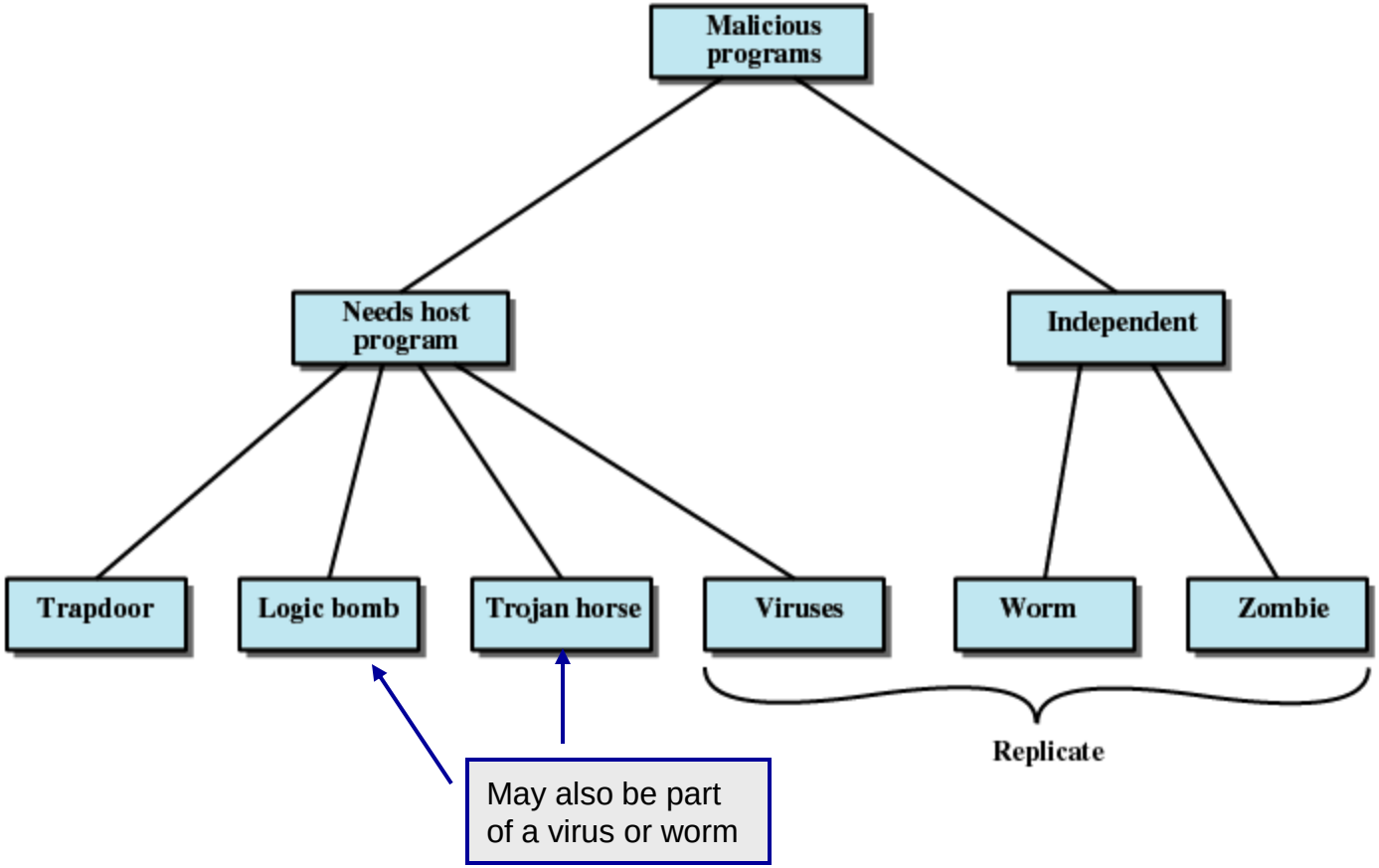
Intrusion Detection (cont.)

- 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

Malicious Programs (Malware)

- Those that need a host program
  - Fragments of programs that cannot exist independently of some application program, utility, or system program.
- Independent
  - Self-contained programs that can be scheduled and run by the operating system.

Malicious Programs (Malware) (cont.)



Taxonomy of Malicious Programs

Trapdoor

- Entry point into a program that allows someone who is aware of trapdoor to gain access.
- Used by programmers to debug and test programs.
  - Avoids necessary setup and authentication.
  - Method to activate program if something goes wrong with authentication procedure.
  - Typically activated via a special sequence of input or is triggered by being run from a certain user ID.
  - Remember the movie "War Games"?

Logic Bomb

- Code embedded in a legitimate program that is set to "explode" when certain conditions are met.
  - Presence or absence of certain files.
  - Particular day of the week.
  - Particular user running application.
- Once triggered, the bomb may alter or delete data or entire files, cause a machine to halt, or do some other damage.
- Case of Tim Lloyd, who was convicted of setting a logic bomb that cost his employer, Omega Engineering, more than $10 million, derailed its corporate growth, and eventually led to the layoff of 80 workers. He was ultimately convicted, sentenced to 41 months in prison and ordered to pay $2 million in restitution.

Trojan Horse

- A useful, or apparently useful, program that contains hidden code that when invoked performs some unwanted or harmful function.
- Can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly.
  - For example, it may set file permission so everyone has access to any file.
  - Modify a compiler to insert additional code into certain programs as they are compiled, such as a system login program. The code creates a trap door in the login program that permits the author to log on to the system using a special password.

Virus

- Program that can "infect" other programs by modifying them; the modification includes a copy of the virus program, which can then go on to infect other programs.
- Lodged in a host computer, a typical virus takes temporary control of the computer's disk operating system. Then, whenever the infected computer comes into contact with an uninfected piece of software, a fresh copy of the virus passes into the new program.
- Thus, the infection can be spread from computer to computer by unsuspecting users who either swap disks or send programs to one another over a network.

Worms

- Use network connections to spread from system to system. Once active in a system, a worm can behave as a virus , or it could implant Trojan horse programs.
- Electronic mail facility
  - A worm mails a copy of itself to other systems.
- Remote execution capability
  - A worm executes a copy of itself on another system.
- Remote log-in capability
  - A worm logs on to a remote system as a user and then uses commands to copy itself from one system to the other.

Zombie

- Program that secretly takes over another Internet-attached computer.
- It uses that computer to launch attacks that are difficult to trace to the zombie's creator.
- Typically, zombies are used in denial-of-service attacks against a targeted website.
- The zombie is planted on hundreds of computers belonging to unsuspecting third parties, and then used to overwhelm the target by launching an overwhelming onslaught of traffic.

The Nature of Viruses

Stages of a virus:

- Dormant phase
  - Virus is idle. Not all viruses have this stage.
- Propagation phase
  - Virus places an identical copy of itself into other programs or into certain system areas on the disk.
- Triggering phase
  - Virus is activated to perform the function for which it was intended.
  - Caused by a variety of system events.
- Execution phase
  - Function is performed.

Types of Viruses

- Parasitic
  - Attaches itself to executable files and replicates.
  - When the infected program is executed, it looks for other executables to infect.
- Memory-resident
  - Lodges in main memory as part of a resident system program.
  - Once in memory, it infects every program that executes.

Types of Viruses (cont.)

- Boot sector
  - Infects boot record.
  - Spreads when system is booted from the disk containing the virus.
- Stealth
  - Specifically designed to hide itself from detection by antivirus software.
  - May use compression so that the infected program is exactly the same length as an uninfected version.

Types of Viruses

- Polymorphic
  - Creates copies during replication that are functionally equivalent but have distinctly different bit patterns.
  - Mutates with every infection, making detection by the "signature" of the virus impossible.
  - Mutation engine creates a random encryption key to encrypt the remainder of the virus.
    - The key is stored with the virus.

Macro Viruses

- In recent years, the number of viruses encountered at corporate sites has risen dramatically. Much of this increase is due to the proliferation of one of the macro viruses. Macro viruses are particularly threatening for a number of reasons:

1. Platform independent.
   - Most infect Microsoft Word documents.
2. Infect documents, not executable portions of code.
3. Easily spread. Commonly via email.

Macro Viruses (cont.)

- A macro is an executable program embedded in a word processing document or other type of file.
- Autoexecuting macros in Word
  - Autoexecute
    - Executes when Word is started
  - Automacro
    - Executes when defined event occurs such as opening or closing a document
  - Command macro
    - Executed when user invokes a command (e.g., File Save)

Antivirus Approaches

- The ideal solution to the threat of viruses is prevention: do not allow a virus to get into the system in the first place.
- This goal is, in general, impossible to achieve, although prevention can reduce the number of successful viral attacks.
- The next best approach is to be able to do the following:
  - Detection – once the infection has occurred, determine that it has occurred an locate the virus.
  - Identification – once detection has been achieved, identify the specific virus that has infected a program.
  - Removal – once the specific virus has been identified, remove all traces of the virus from the infected program and restore it to its original state.

Generic Decryption

- Since a polymorphic virus is typically encrypted, GD technology passes all executable files through a GD scanner, which includes the following elements:
  - CPU emulator
    - Instructions in an executable file are interpreted by the emulator rather than the processor.
  - Virus signature scanner
    - Scan target code looking for known virus signatures.
  - Emulation control module
    - Controls the execution of the target code .

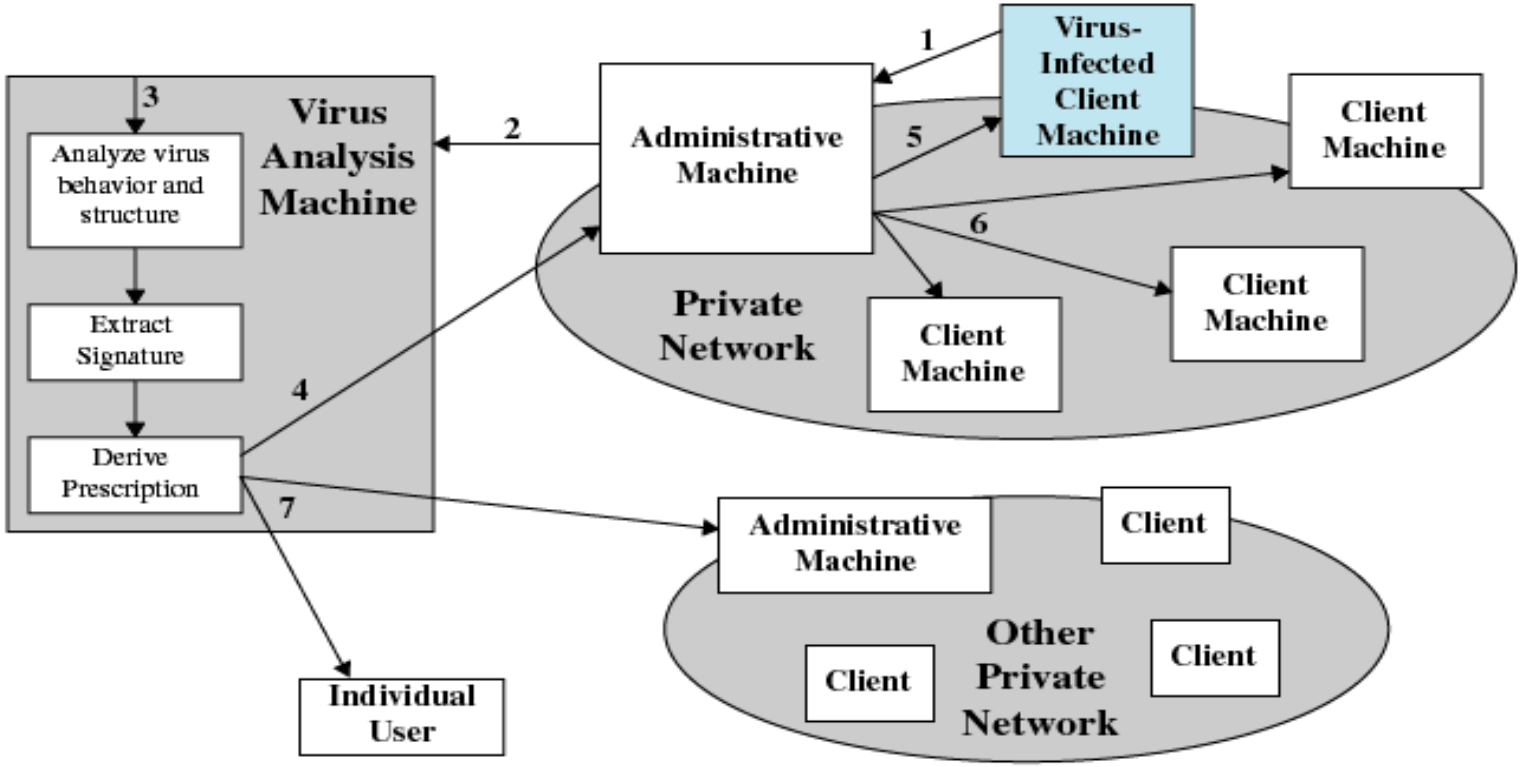
Digital Immune System

- A comprehensive approach to virus protected developed by IBM.
- Motivation has been the rising threat of Internet-based virus propagation
  - Integrated mail systems
  - Mobile-program system

Digital Immune System – How It Works

1. A monitoring program on each computer uses a variety of heuristics based on system behavior, suspicious changes to programs, or family signature to infer that a virus may be present. The monitoring program forwards a sample copy of any program thought to be infected to an administrative machine.
2. The administrative machine encrypts the sample and sends it to a central virus analysis machine.
3. This machine creates an environment in which the infected program can be run for analysis. The virus analysis machine then produces a prescription for identifying and removing the virus.
4. The resulting prescription is sent back to the administrative machine.
5. The administrative machine forwards the prescription to the infected client.
6. The prescription is also forwarded to other clients in the organization.
7. Subscribers around the world receive regular antivirus updates that protect them from the new virus.

Digital Immune System – How It Works (cont.)



Digital Immune System

E-mail Virus

- Activated when recipient opens the e-mail attachment.
- Activated by opening an e-mail that contains the virus.
- Uses Visual Basic scripting language.
- Propagates itself to all of the e-mail addresses known to the infected host.