System Security

Contents

- Intrusion and intruder
- Intrusion techniques
- Intrusion prevention and detection
- Password management
- Password selection strategies
- How to choose secure password
- Virus and threats
- Virus Countermeasures

Intruders

Also known as hackers or crackers

One of the most publicized threats to security

- significant problem of networked systems
  - hostile/unwanted trespass
  - from benign to serious
- user trespass
  - unauthorized logon, privilege abuse
- software trespass
  - virus, worm, or Trojan horse

Intruders

- Attacks range from harmless to devastating
  - Some just want to explore
  - Some read or modify sensitive data or cause disruptions
- No way to tell in advance how harmful an intruder will be
  - Any intruder must be considered a threat

Intruders

Three classes:

- **Masquerader:** Someone not authorized to use a computer; penetrates access controls to exploit a legitimate account
- **Misfeasor:** A legitimate user who accesses unauthorized resources or misuses privileges
- **Clandestine user:** Someone who gains supervisory control and evades or suppresses auditing and access controls

Example

- Texas A&M University in 1992
  - Received notification that one of their computers was attacking computers at a different location
  - Several outside intruders involved
  - The machines were disconnected by the university and security holes were patched
  - A few days later, attacks resumed
  - Found hundreds of captured passwords in files
  - Found a bulletin board (on one of their machines) used by hackers for discussion of techniques and progress

Intruder Types and Behaviors

- Three broad categories
  - Hackers
  - Criminals
  - Insiders

Hackers

- motivated by “thrill” and “status/reputation”
  - hacking community is a strong meritocracy
  - status is determined by level of competence
- benign intruders might be tolerable
  - do consume resources and may slow performance
  - can’t know in advance whether benign or malign

What to do

  - IDS (Intrusion Detection Systems), IPS (Intrusion Prevention System), VPNs can help to counter
- Awareness of intruder problems led to establishment of CIRTs
  - Computer/Cyber Incident Response Teams
  - collect / disseminate vulnerability info / responses

Criminals / Criminal Enterprises

- the main motivation is to make money
- the common threat is *organized groups of cyber criminals*
  - May be employed by a corporation / government
  - Most of the time, loosely affiliated gangs
  - Typically young
  - often Eastern European, Russian, Southeast Asian
- common target is financial institutions, bank accounts and credit cards on e-commerce servers
- criminal hackers usually have specific targets
- once penetrated act quickly and get out
- IDS may help but less effective due to quick-in-and-out strategy
- sensitive data needs strong data protection (e.g. credit card numbers)
- Strong authentication would also help (2-factor auth.)

Insider Attacks

- Most difficult to detect and prevent
  - employees have access & system knowledge
- Attackers are motivated by revenge / feeling of entitlement
  - when employment terminated
  - taking customer data when moving to competitor
- IDS/IPS may help but also need extra precautions
  - least privilege (need-to-know basis)
  - monitor logs
  - DLP (data loss prevention) tools – sw agents monitoring user behaviors
  - Upon termination revoke all rights and network access

Insider Behavior Example

1. create accounts for themselves and their friends
2. access accounts and applications they wouldn't normally use for their daily jobs
3. conduct furtive instant-messaging chats
4. visit web sites that cater to disgruntled employees
5. perform large downloads, file copying and printing
6. access the network during off hours.

Intrusion

- An *intrusion* is a deliberate unauthorized attempt, successful or not, to break into, access, manipulate, or misuse some valuable property and where the misuse may result into or render the property unreliable or unusable.
- The person who intrudes is an *intruder*.

Intrusion

- Entrance by force or without permission or welcome.
- Any set of actions that attempt to compromise the **integrity, confidentiality or availability** of a resource.
- The intentional insertion of electromagnetic energy into transmission paths in any manner with the objective of deceiving operators or of causing confusion.

Intrusion techniques

- Objective:
  - Gain access to a system
  - Or, gain more privileges on a system
- Generally requires the intruder to access protected information
  - Most likely, a password to a user's account
- Password file
  - Passwords may be hashed (one-way function)
  - Or, may only be accessible by certain accounts

Intrusion techniques

- Learning a password
  - Try default passwords for the system
  - Guess
    - Brute force it
    - Dictionary words
    - Commonly used passwords (e.g., “password”, “admin”)
    - Personal information about user (e.g., name, address, phone number)
  - Trojan horse to bypass security
  - Tap line between user and system

Intrusion techniques

- Exploit security holes
  - Buffer overflows in a program running with privileges
    - Run unauthorized instructions
  - System does not check for invalid user input
    - Disrupts data integrity
    - Also run unauthorized instructions
  - Software bugs

Examples of Intrusion

- remote root compromise
- web server defacement
- guessing / cracking passwords
- copying / viewing sensitive data / databases
- running a packet sniffer to obtain username/passwords
- impersonating a user to reset/learn password
  - Mostly via social engineering, phishing
- using an unattended and logged-in workstation

Intrusion detection

- Intrusion detection is a technique of detecting unauthorized access to a computer system or a computer network.
- An intrusion into a system is an attempt by an outsider to the system to illegally gain access to the system.
- Intrusion prevention, on the other hand, is the art of preventing an unauthorized access of a system's resources.
- The two processes are related in a sense that while intrusion detection passively detects system intrusions, intrusion prevention actively filters network traffic to prevent intrusion attempts.

Intrusion Detection Systems (IDSs)

- An *intrusion detection system (IDS)* is a system used to detect unauthorized intrusions into computer systems and networks.
- Intrusion detection as a technology is not new, it has been used for generations to defend valuable resources.
- These are three models of intrusion detection mechanisms: *anomaly-based* detection, *signature-based* detection, and *hybrid* detection.

Intrusion detection approaches

- **Statistical anomaly detection:** Involves the collection of data **relating to the behavior** of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.

Intrusion detection approaches

- **Rule-based detection:** Involves an attempt to define **a set of rules** that can be used to decide that a given behavior is that of an intruder.

Security Intrusion and Intrusion Detection – Def'ns from RFC 2828

Security Intrusion

> a security event, or combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so.

Intrusion Detection

> a security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner.

Intrusion detection

- Motivated by:
  - If the intruder can be detected and ejected quickly, damage to the system is minimized
  - If effective, acts as a deterrent
  - Collecting information about intrusion techniques
- Based on assumption that an intruder behaves differently than a legitimate user
  - Behaviour overlaps
  - Potential for false positives or negatives

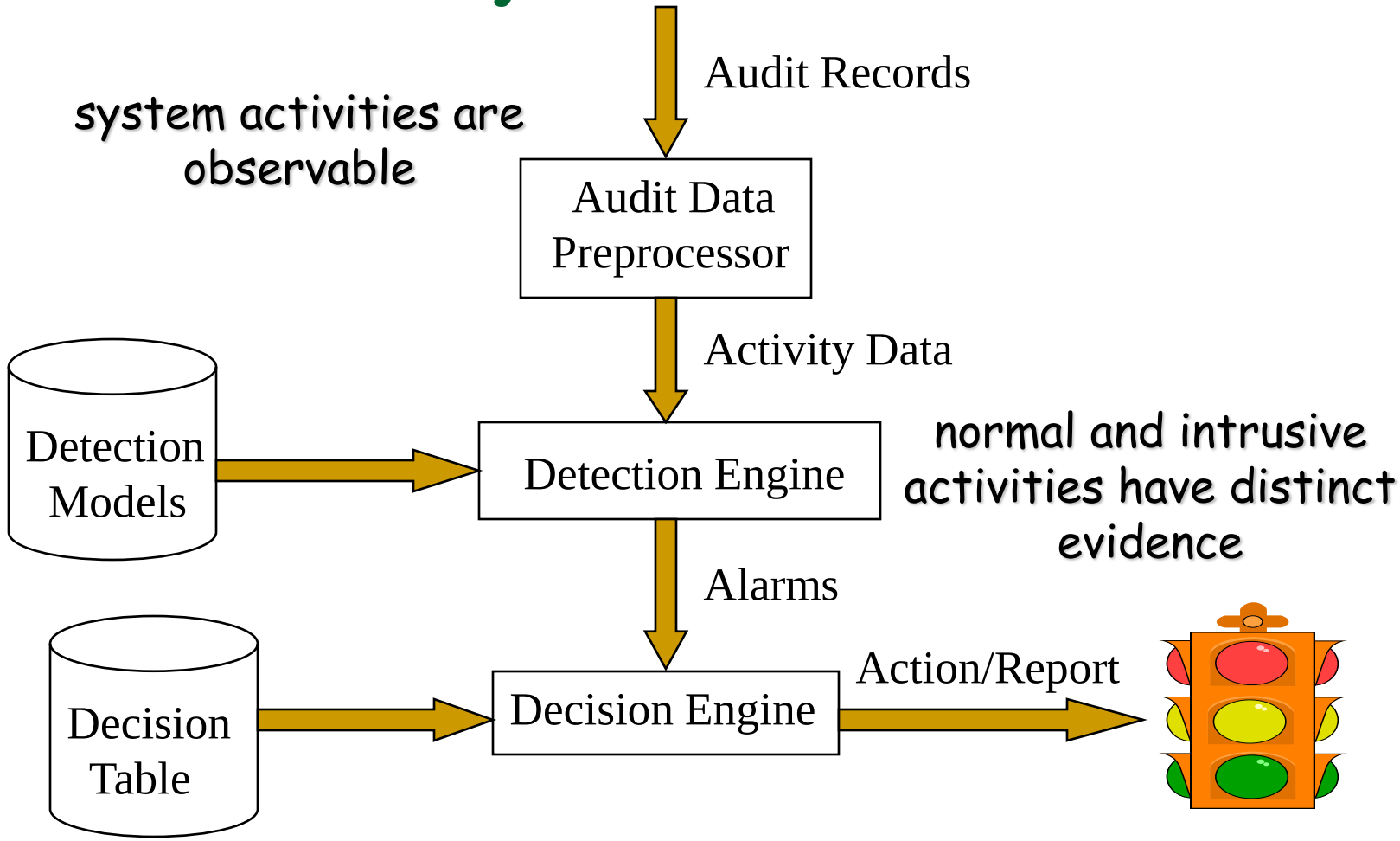
Intrusion detection

- Balancing act
  - Strong detection… Many false alarms; system managers will ignore
  - Weak detection… False sense of security
- Two approaches:
  - Statistical anomaly detection
  - Rule-based detection

Elements of Intrusion Detection

- Primary assumptions:
  - System activities are observable
  - Normal and intrusive activities have distinct evidence
- Components of intrusion detection systems:
  - From an algorithmic perspective:
    - Features - capture intrusion evidences
    - Models - piece evidences together
  - From a system architecture perspective:
    - Audit data processor, knowledge base, decision engine, alarm generation and responses

Components of Intrusion Detection System



Audit records

A fundamental tool for intrusion detection and also a record of user activity that is used as input to an intrusion detection system

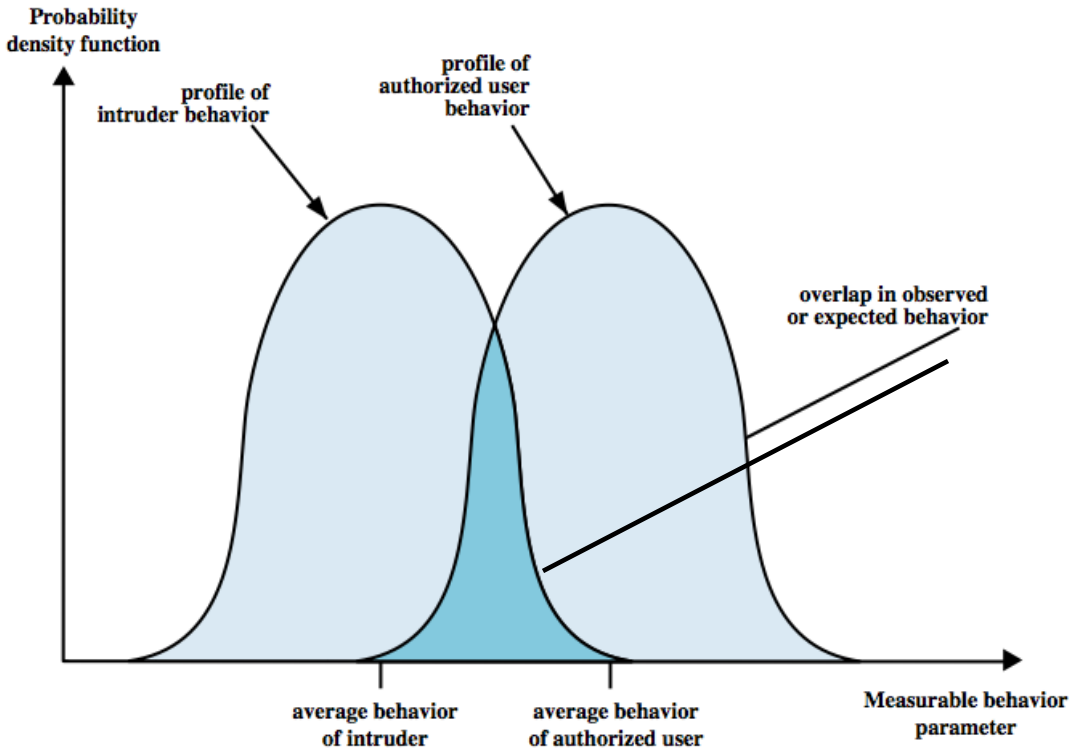
Two types:

- **Native**
  - Information collected by operating system
  - always available but may not contain relevant information or may not be in convenient form
- **Detection-specific**
  - Facility implemented that collects information only needed by detection system
  - Extra overhead due to having multiple collection systems in place
  - Example fields:

    Subject, action, object (recipient), exception condition, resource usage, timestamp

IDS Principle

- Main assumption: intruder behavior differs from legitimate user behavior
  - expect overlaps as shown
  - problems
    - false positives: authorized user identified as intruder
    - false negatives: intruder not identified as intruder



IDS Requirements

- run continually with minimal human supervision
- be fault tolerant
- resist subversion
- minimal overhead on system
- scalable, to serve a large numbe of users
- configured according to system security policies
- allow dynamic reconfiguration

Intrusion Detection Systems (IDS)

- IDS classification
  - Host-based IDS: monitor single host activity
  - Network-based IDS: monitor network traffic
- logical components:
  - Sensors
    - collect data from various sources such as log files, network packets
    - sends them to the analyzer
  - Analyzers
    - process data from sensors and determine if intrusion has occurred
    - may also provide guidance for the actions to take
  - user interface
    - acts as a console
    - view the output and manage the behavior

Host-Based IDS

- specialized software to monitor system activity to detect suspicious behavior
  - primary purpose is to detect intrusions, log suspicious events, and send alerts
  - can detect both external and internal intrusions
- two approaches, but often used in combination:
  - **signature detection**
    - attack patterns are defined and they are used to decide on intrusion
  - **anomaly detection**
    - collection of data related to the behavior of legitimate users
    - Statistical tests are applied to observed behavior
      - threshold detection – applies to all users
      - profile based – differs among the users

Signature Detection

- Observe events on system and applying a set of rules to decide if intruder
- Approaches:
  - rule-based anomaly detection
    - analyze historical audit records for expected behavior, then match with current behavior
  - rule-based penetration identification
    - rules identify known penetrations or possible penetrations due to known weaknesses
    - rules are mostly OS specific
    - rules obtained by analyzing attack scripts from Internet
      - supplemented with rules from security experts of target system

Anomaly Detection

- Threshold detection
  - Checks excessive event occurrences over time
  - Crude and ineffective intruder detector per se
  - Creates lots of false positives/negatives due to
    - Variance in time
    - Variance accross users
- Profile based
  - Characterize past behavior of users and groups
  - Then, detect significant deviations
  - Based on analysis of audit records
    - example metrics: counter, guage, interval timer, resource utilization
    - analysis methods: mean and standard deviation, multivariate, markov process, time series

Profile based Anomaly Detection - Analysis Methods

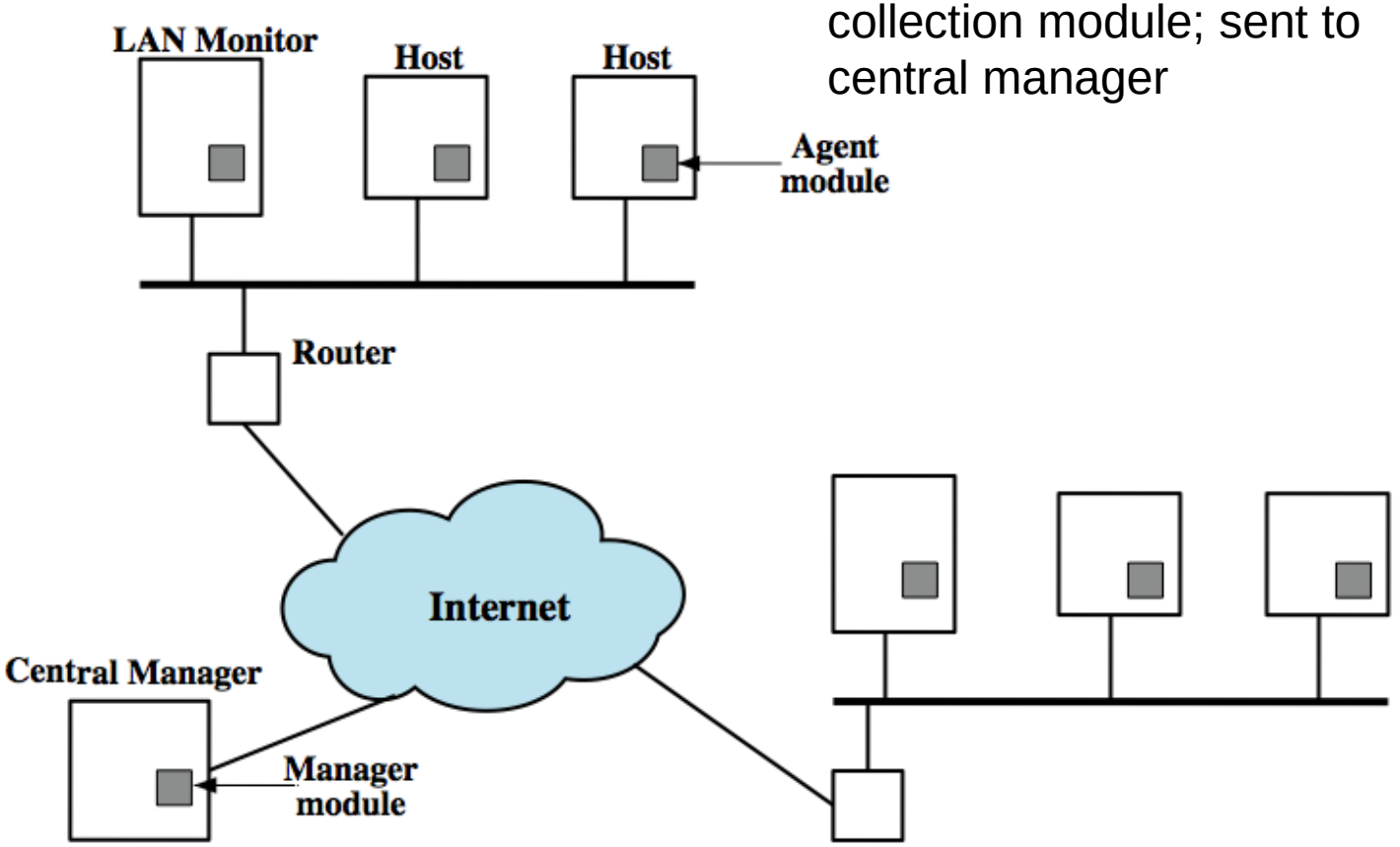
- Mean and standard deviation
  - of a particular parameter
  - Not good (too crude)
- Multivariate analysis
  - Correlations among several parameters (ex. relation between login freq. and session time)
- Markov process
  - Considers transition probabilities
- Time series analysis
  - Analyze time intervals to see sequences of events happening rapidly or slowly
- All statistical methods using AI, Mach. Learning and Data Mining techniques.

Distributed Host-Based IDS

main idea: coordination and cooperation among IDSs across the network

Host agent module: audit collection module; sent to central manager

LAN Monitor agent module: analyze LAN traffic and send to Central Manager



Central Manager Module: Analyze and correlate data received from other modules

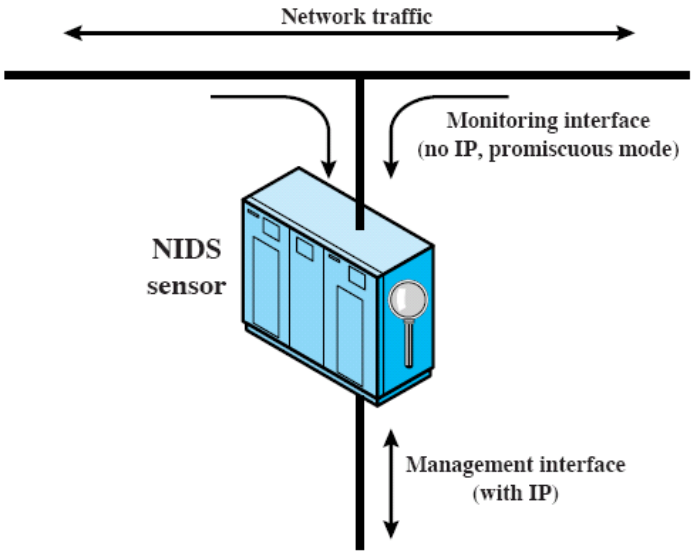
Architecture

Network-Based IDS

- network-based IDS (NIDS)
  - monitor traffic at selected points on a network to detect intrusion patterns
    - in (near) real-time
  - may examine network, transport and/or application level protocol activity directed toward the system to be protected
    - Only network packets, no software activity examined
- System components
  - A number of sensors to monitor packet traffic
  - Management server(s) with console (GUI)
- Analysis can be done at sensors, at management servers or both

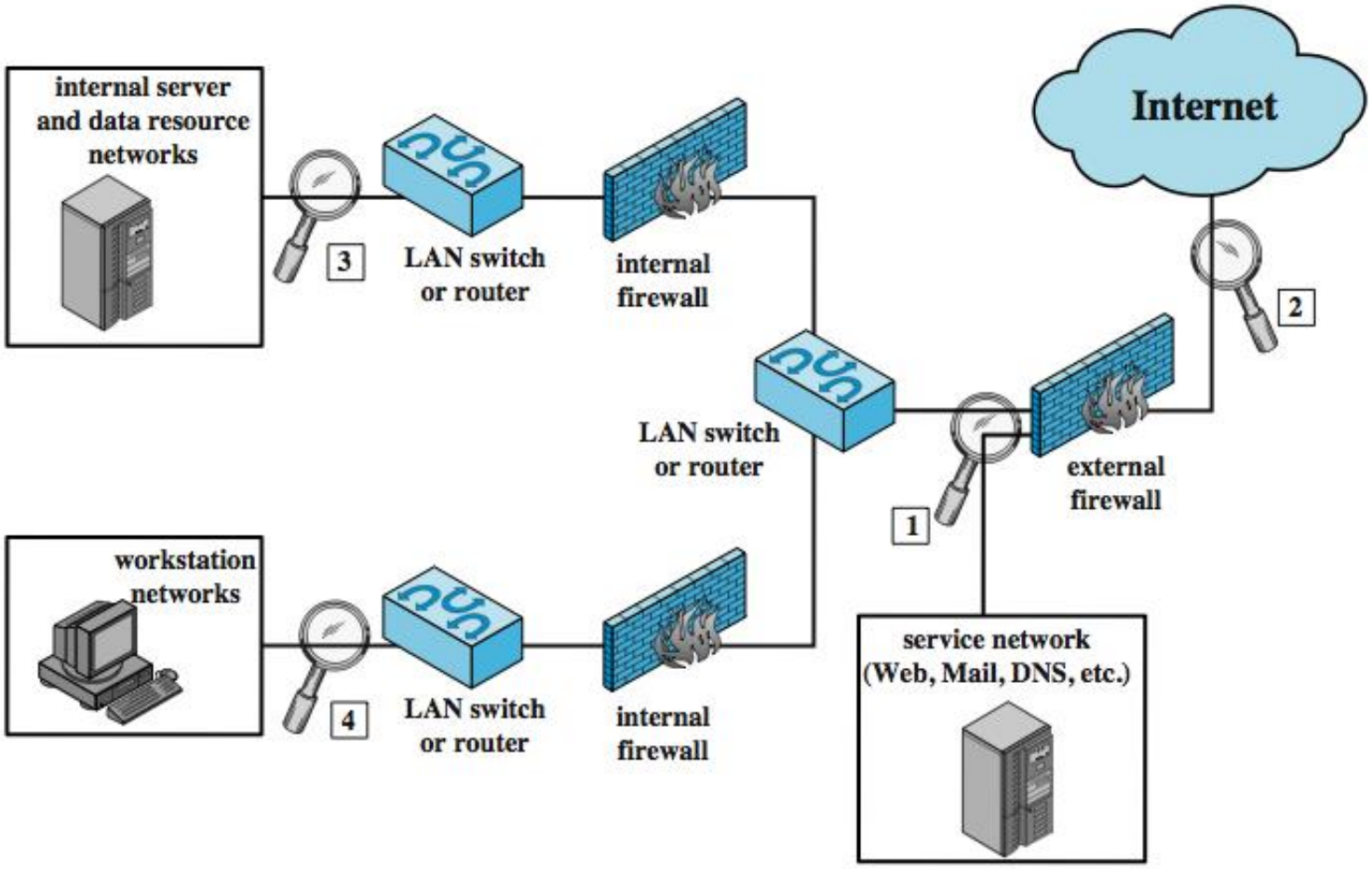
Network-Based IDS

- Types of sensors
  - inline and passive
- Inline sensors
  - Inserted into a network segment
  - Traffic pass through
  - possibly as part of other networking device (e.g. router, firewall)
    - No need for a new hardware; only new software
  - May create extra delay
  - Once attack is detected, traffic is blocked
    - Also a prevention technique
- Passive sensors
  - monitors copy of traffic at background
    - Traffic does not pass through it, so there is no blocking capability
  - More efficient, therefore more common



Passive sensor

NIDS Sensor Deployment



Intrusion Detection Techniques in NIDS

- signature detection
  - at application (mostly), transport, and network layers
  - Attack patterns are detected in packets
- anomaly detection – attacks that cause abnormal behaviors are detected
  - denial of service attacks, scanning attacks
- when potential violation detected, sensor sends an alert and logs information

Rule-based detection

- Attempts to define a set of rules with regards to what is legitimate or intrusive behaviour

Rule-based detection

Two categories:

- Anomaly detection
  - Similar to statistical anomaly detection
  - Usage patterns are identified and rules are generated to describe such patterns in behaviour
  - Current behaviour is observed and compared to past behaviour
- Penetration identification
  - Rules are defined with regards to known penetrations, ways to exploit system weaknesses, and suspicious behaviour
  - Rules are generated by experts; interviews are conducted with administrators, security analysts, or hackers themselves

Distributed intrusion detection

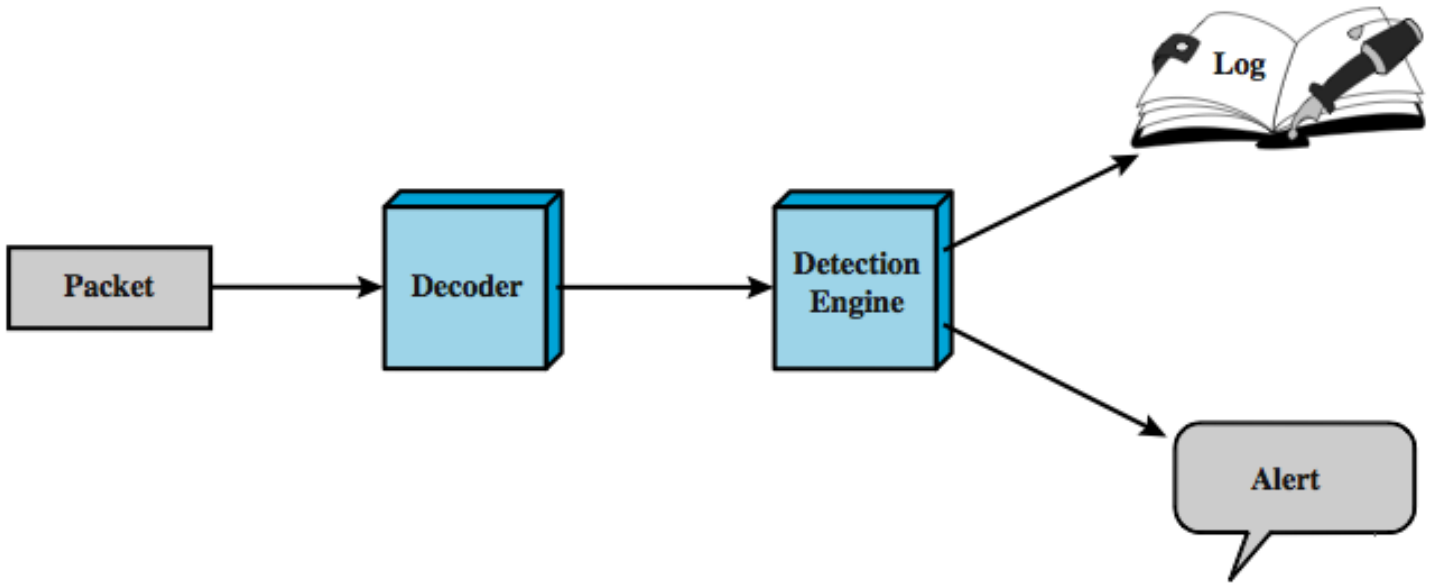
- A detection system that monitors behaviour across a network of systems
- Major issues to consider:
  - May need to deal with multiple formats of audit records
  - Audit records will need to be transferred through the network to a node with the detection system
    - Data integrity and confidentiality
  - Centralization
    - One node… Single point of failure
    - Many nodes… Must coordinate

An Example IDS: Snort

- Lightweight IDS
  - open source
  - Portable, efficient
  - easy deployment and configuration
  - May work in host-based and network-based manner
- Snort can perform
  - real-time packet capture and rule analysis
- Sensors can be inline or passive
  - In inline case, Snort can also be used as IPS

Snort Architecture

- Packet Decoder: parses the packet headers in all layers
- Detection Engine: actual IDS. Rule-based analysis.
- If the packet matches a rule, the rule specifies logging and alerting options



SNORT Rules

- Snort uses a simple, flexible and effective rule definition language
  - But needs training to be an expert on it
- Each rule has a fixed header and zero or more options
- Header fields
  - action: what to do if matches – alert, drop, pass, etc.
  - protocol: analyze further if matches - IP, ICMP, TCP, UDP
  - source IP: single, list, any, negation
  - source port: TCP or UDP port; single, list, any, negation
  - direction: unidirectional (->) or bidirectional (<->).
  - dest IP, dest port: same format as sources

Intrusion Prevention Systems (IPS)

- Later addition to terminology of security products
- Two Interpretations of IPS
  - inline network or host-based IDS that can block traffic
  - functional addition IDS capabilities to firewalls
- An IPS can block traffic like a firewall, but using IDS algorithms
  - may be network or host based
- Inline Snort is actually an IPS

Intrusion Prevention Systems (IPSs)

- Although IDS have been one of the cornerstones of network security, they have covered only one component of the total network security picture since they have been and they are a passive component which only detects and reports without preventing.
- A promising new model of intrusion is developing and picking up momentum. It is the *intrusion prevention system* (IPS) which, is to prevent attacks.
- Like their counterparts the IDS, IPS fall into two categories: network-based and host-based.

Network-Based Intrusion Prevention Systems (NIPSs)

- Because **NIDSs are passively detecting intrusions into the network without preventing them from entering the networks,** many organizations in recent times have been **bundling up IDS and firewalls to create a model that can detect and then prevent**.

- The bundle works as follows.
  - The IDS fronts the network with a firewall behind it. On the detection of an attack, the IDS then goes into the prevention mode by altering the firewall access control rules on the firewall. The action may result in the attack being blocked based on all the access control regimes administered by the firewall.

  - The IDS can also affect prevention through the TCP resets; TCP utilizes the RST (reset) bit in the TCP header for resetting a TCP connection, usually sent as a response request to a non-existent connection.

Host-Based Intrusion Prevention Systems (HIPSs)

- Most HIPSs work by *sand-boxing*, a process of restricting the definition of acceptable behavior rules used on HIPSs. HIPS prevention occurs at the agent residing at the host.
- The agent intercept system calls or system messages by utilizing dynamic linked libraries (dll) substitution.
- The substitution is accomplished by injecting existing system dlls with vendor stub dlls that perform the interception.

Honeypots

- A *honeypot* is a system designed to look like something that an intruder can hack.
- They are built for many purposes but the overriding one is to deceive attackers and learn about their tools and methods.
- Honeypots are also add-on/tools that are not strictly sniffer-based intrusion detection systems like HIDS and NIDS. However, they are good deception systems that protect the network in much the same way as HIDS and NIDS.
- Since the goal for a honeypot is to deceive intruders and learn from them without compromising the security of the network, then it is important to find a strategic place for the honeypot.

Honeypots

- two primary **types** of **honeypot** designs:
  - Production **honeypots**—serve as decoy systems inside fully operating networks and servers, often as part of an intrusion detection system (IDS).
  - Research **honeypots**—used for educational purposes and security enhancement.

Need for Password

- because of the widespread adoption of computer networks, and particularly the Internet, has enabled electronic access to almost every possible service: e-mail, e-commerce, banking and government services.
- But with this access has come the need to identify the users of these services, both to safeguard personal information and to control the capabilities given to each user.
- An encrypted password database is likely to be much more secure than a notebook or a wallet.

Need for Password

- Because of the difficulties associated with remembering passwords, a group of software applications, called password keepers or password managers has emerged.
- These applications deal with everything from the simple storage of user IDs and passwords to the management of password access across many users.
- Poor encryption or use of a weak master password, allowing the contents to be accessed.

Password management

- A password system is almost always the front line of defense
- Each user has a username (or ID) and password
  - Username determines what privileges that user has
  - A guest or anonymous account may also exist with very limited privileges
  - Password is used for authentication when logging in

Password Management

- **Password Protection:**
  - The front line of defense against intruders is the password system.
  - Virtually all multiuser systems require that a user provide not only a name or identifier (ID) but also a password.
  - The password serves to authenticate the ID of the individual logging on to the system.

Password Management

- The ID determines whether the user is authorized to gain access to a system.
- The ID determines the privileges accorded to the user.

Password vulnerabilities

- A password file typically does not store passwords as plaintext
  - A unique salt (e.g., username) is attached to a user's password, encrypted using some algorithm, then stored
  - Having obtained the password file, an intruder would need to decrypt the passwords contained in it…not necessarily an easy task
- This is fine, but…if someone's password is "password", it doesn't matter how secure your password file is

Password vulnerabilities

Some people choose passwords that are easy to guess

- Dictionary words
- Personal information

Or, too short in length

- System may enforce a minimum length

Strategy to obtain a password

- Try personal information
- Try dictionary words
- Try exchanging letters with lookalike symbols (e.g., letter O with number zero)
- Try varying capitalization

This allows for a password to be obtained without having to actually decrypt it the password file

Password vulnerabilities

- Password file is most likely only accessible by certain accounts
- Some users may use the same password for a variety of systems
  - Intruder may obtain their password from one system and try it on another

Password selection

- Users may choose a password that is easy to remember…insecure because easily guessable
- System may assign a randomly generated password…secure, but not easy to remember
- Goal: generate a password that is not easy to guess, but is easy to remember

Password selection

Password Selection Strategies: The goal is to eliminate guessable passwords while allowing the user to select a password that is memorable. Four basic techniques are in use:

- **User education:** Users can be told the importance of using hard-to-guess passwords and can be provided with guidelines for selecting strong passwords.
- **Computer-generated passwords:** Use an algorithm (e.g., produce a password with pronounceable syllables) to generate a user's password and are quite random in nature

Password Management

- **Reactive password checking**
  - the system periodically runs its own password checker and cracker to find guessable or weak passwords. The system cancels any passwords that are guessed
- **Proactive password checking**
  - user is allowed to select his or her own password. However, at the time of selection, the system checks to see if the password is allowable and, if not, rejects it.
  - The trick with a proactive password checker is to strike a balance between user acceptability and strength.

Password Management

- **Proactive password checking approaches:**
  - Rule enforcement:
    - All passwords must be at least eight characters long.
    - The passwords must include at least one each of uppercase, lowercase, numeric digits, and punctuation marks.
  - Another possible procedure is simply to compile a large dictionary of possible "bad" passwords.

Password Management

- **Proactive password checker techniques**
  - Markov model: generation of guessable passwords, this model shows a language consisting of an alphabet of three characters. The state of the system at any time is the identity of the most recent letter. The value on the transition from one state to another represents the probability that one letter follows another. Thus, the probability that the next letter is b, given that the current letter is a, is 0.5.

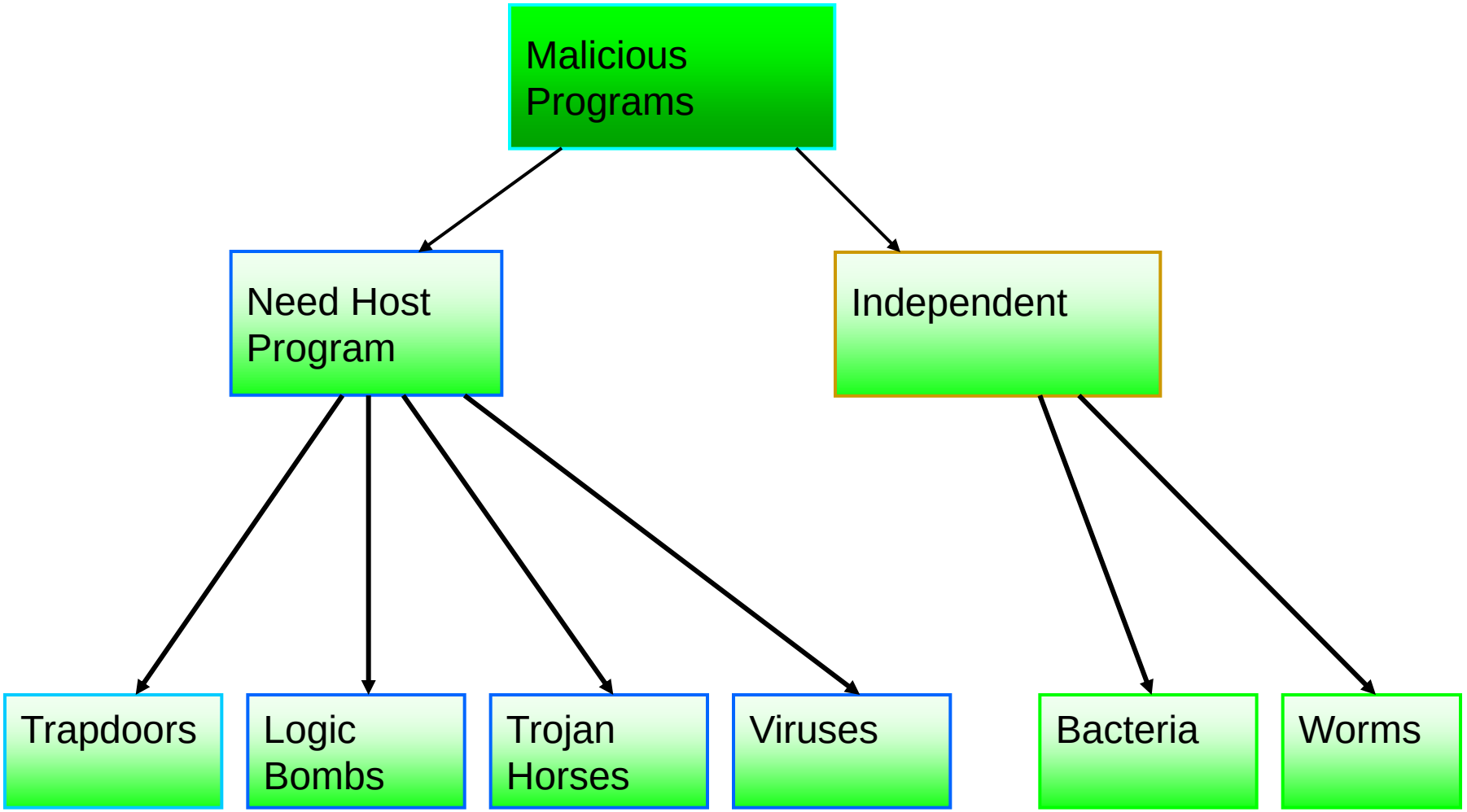
How to Choose a secure password?

- Do NOT use words or phrases that have personal significance.
- Mix letters, numbers and symbols, and use case sensitivity
- Try to memorize the password, and avoid writing it down
- Do not use the same password for everything
- Use a password manager (PM). It is a utility that creates an encrypted file where your passwords are stored.
- Try to use "nonsense words."
- Do not tell anybody your password.

Viruses and ”Malicious Programs”

- Computer “Viruses” and related programs have the ability to replicate themselves on an ever increasing number of computers. They originally spread by people sharing floppy disks. Now they spread primarily over the Internet (a “Worm”).
- Other “Malicious Programs” may be installed by hand on a single machine. They may also be built into widely distributed commercial software packages. These are very hard to detect before the payload activates (Trojan Horses, Trap Doors, and Logic Bombs).

Taxanomy of Malicious Programs



Definitions

- Virus - code that copies itself into other programs.
- A “Bacteria” replicates until it fills all disk space, or CPU cycles.
- Payload - harmful things the malicious program does, after it has had time to spread.
- Worm - a program that replicates itself across the network (usually riding on email messages or attached documents (e.g., macro viruses).

Definitions

- Trojan Horse - instructions in an otherwise good program that cause bad things to happen (sending your data or password to an attacker over the net).
- Logic Bomb - malicious code that activates on an event (e.g., date).
- Trap Door (or Back Door) - undocumented entry point written into code for debugging that can allow unwanted users.
- Easter Egg - extraneous code that does something "cool." A way for programmers to show that they control the product.

Virus Phases

- **Dormant phase** - the virus is idle
- **Propagation phase** - the virus places an identical copy of itself into other programs
- **Triggering phase –** the virus is activated to perform the function for which it was intended
- **Execution phase** – the function is performed

Types of Viruses

- **Parasitic Virus** - attaches itself to executable files as part of their code. Runs whenever the host program runs.
- **Memory-resident Virus** - Lodges in main memory as part of the residual operating system.
- **Boot Sector Virus** - infects the boot sector of a disk, and spreads when the operating system boots up (original DOS viruses).
- **Stealth Virus** - explicitly designed to hide from Virus Scanning programs.
- **Polymorphic Virus** - mutates with every new host to prevent signature detection.

Macro Viruses

- Microsoft Office applications allow “macros” to be part of the document. The macro could run whenever the document is opened, or when a certain command is selected (Save File).
- Platform independent.
- Infect documents, delete files, generate email and edit letters.

Antivirus Approaches

1st Generation, Scanners: searched files for any of a library of known virus “signatures.” Checked executable files for length changes.

2nd Generation, Heuristic Scanners: looks for more general signs than specific signatures (code segments common to many viruses). Checked files for checksum or hash changes.

3rd Generation, Activity Traps: stay resident in memory and look for certain patterns of software behavior (e.g., scanning files).

4th Generation, Full Featured: combine the best of the techniques above.

Advanced Antivirus Techniques

- Generic Decryption (GD)
  - CPU Emulator
  - Virus Signature Scanner
  - Emulation Control Module