Info Security Technology

Topic 4

Network Security

(Part III)

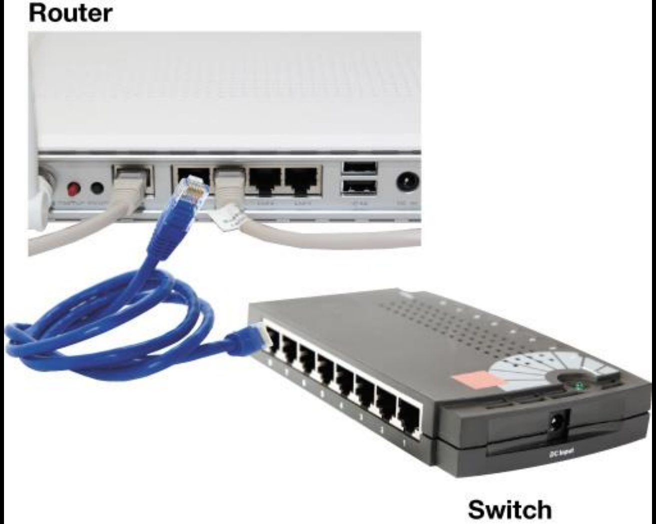
Objectives

- Able to describe the different methods of wireless attacks.
- List the different types of Intrusion Detection System (IDS).
- Compare and firewall with IDS.

Wireless Network Attack

Connecting Devices to a Router

- Routers for Windows computers
  - 802.11n
  - 802.11ac



- Routers for Apple computers
  - AirPort Extreme router
  - AirPort Express

Network-Attached Storage Devices

- NAS devices
- AirPort Time Capsule

Specialized Home-Networking Devices

- New digital picture frames
  - Built-in wireless
  - Access network and online photos
  - Receive pictures via e-mail

- Security
  - Wireless monitoring cameras

Securing Wireless Networks

- Wireless vs Wired Network
- Added vulnerabilities for wireless:
  - Signal range can extend to neighbors
  - Extra precautions required to secure wireless

IEEE 802.11 Wireless LAN

- 802.11b
  - up to 11 Mbps
- 802.11a
  - up to 54 Mbps
- 802.11g
  - up to 54 Mbps
- 802.11n
  - up to 150 ~ 600 Mbps
- All have base-station and ad-hoc network versions

Wireless Network Vulnerabilities

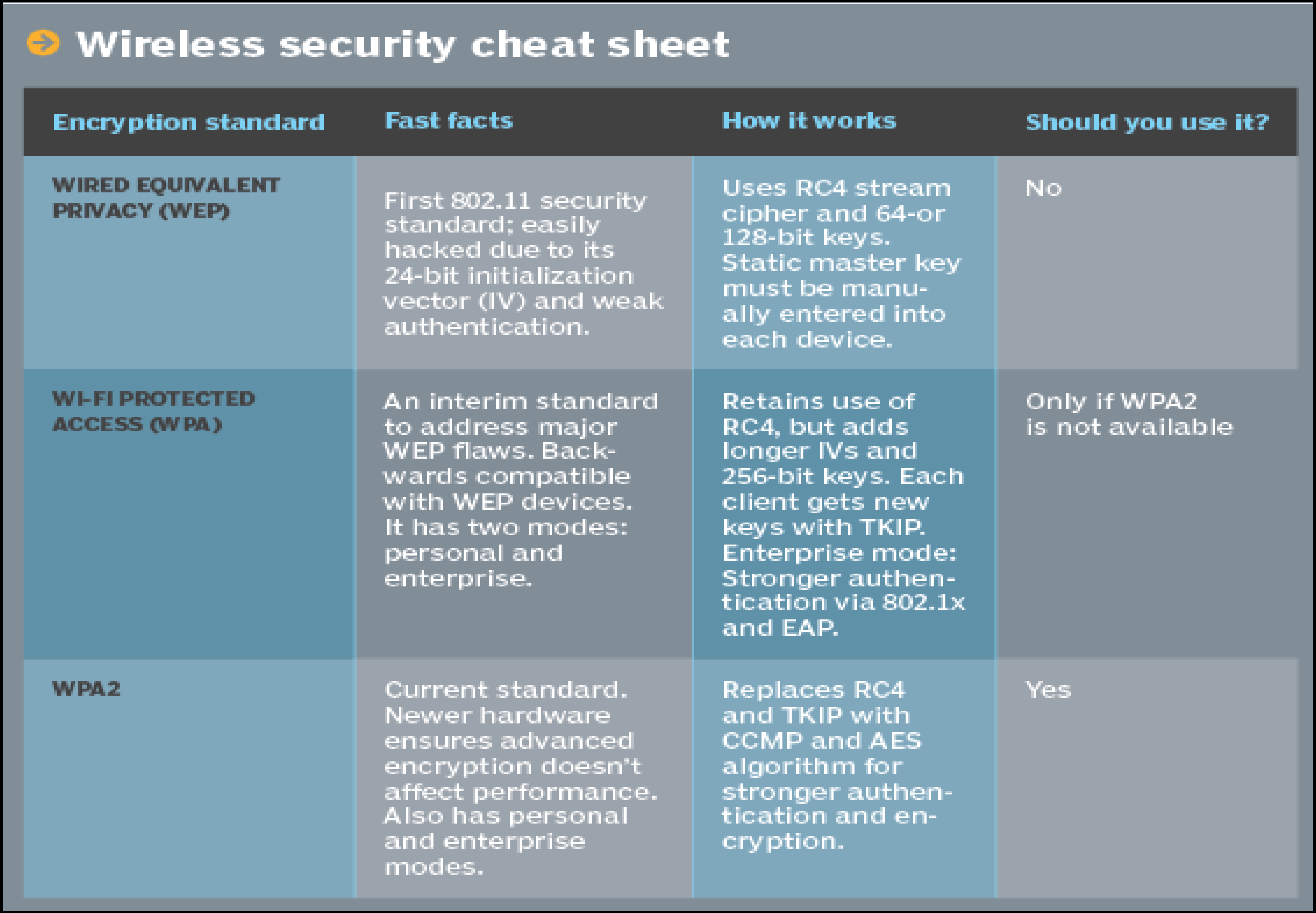
- Early wireless networking standards had vulnerabilities which could be divided into 3 categories:
  - MAC address substitution
    - Addresses exchanged in unencrypted format
    - Attacker can see address of approved device and substitute it on his own device
  - SSID (Service Set Identifier) broadcast
    - Authentication is based only on match of SSIDs
    - Attacker can wait for the SSID to be broadcast by the AP
  - Wired Equivalent Privacy (WEP)
    - WEP can only use 64-bit or 128-bit number to encrypt
    - Short length makes it easier to break
    - Can be overcome by using Wi-Fi Protected Access 2 (WPA2)

802.11b: Built in Security Features

- Service Set Identifier (SSID)
- Differentiates one access point from another
- SSID is cast in ‘beacon frames’ every few seconds.
- Beacon frames are in plain text!

Wired Equivalent Protocol (WEP)

- Primary built security for 802.11 protocol
- Uses 64/128bits RC4 encryption
- Intended to make wireless as secure as a wired network
- Unfortunately, since ratification of the 802.11 standard, RC4 has been proven insecure, leaving the 802.11 protocol wide open for attack



Wireless security cheat sheet

Encryption standard	Fast facts	How it works	Should you use it?
WIRED EQUIVALENT PRIVACY (WEP)	First 802.11 security standard; easily hacked due to its 24-bit initialization vector (IV) and weak authentication.	Uses RC4 stream cipher and 64-or 128-bit keys. Static master key must be manually entered into each device.	No
WI-FI PROTECTED ACCESS (WPA)	An interim standard to address major WEP flaws. Backwards compatible with WEP devices. It has two modes: personal and enterprise.	Retains use of RC4, but adds longer IVs and 256-bit keys. Each client gets new keys with TKIP. Enterprise mode: Stronger authentication via 802.1x and EAP.	Only if WPA2 is not available
WPA2	Current standard. Newer hardware ensures advanced encryption doesn't affect performance. Also has personal and enterprise modes.	Replaces RC4 and TKIP with CCMP and AES algorithm for stronger authentication and encryption.	Yes

Wi-Fi Protected Access (WPA)

- Flaws in WEP known since January 2001 - flaws include weak encryption (keys no longer than 40 bits), static encryption keys, lack of key distribution method.
- In April 2003, the Wi-Fi Alliance introduced an interoperable security protocol known as WiFi Protected Access (WPA).
- WPA was designed to be a replacement for WEP networks without requiring hardware replacements.
- *WPA provides stronger data encryption (weak in WEP) and user authentication (largely missing in WEP).*

WPA Security Enhancements

- WPA includes Temporal Key Integrity Protocol (TKIP) and 802.1x mechanisms.
- The combination of these two mechanisms provides dynamic key encryption and mutual authentication
- TKIP adds the following strengths to WEP:
  - Per-packet key construction and distribution:

    WPA automatically generates a new unique encryption key periodically for each client. This avoids the same key staying in use for weeks or months as they do with WEP.
  - Message integrity code: guard against forgery attacks.
  - 48-bit initialization vectors, use one-way hash function instead of XOR

WPA2

- In July 2004, the IEEE approved the full IEEE 802.11i specification, which was quickly followed by a new interoperability testing certification from the WiFi Alliance known as WPA2.
- Strong encryption and authentication for infrastructure and ad-hoc networks (WPA1 is limited to infrastructure networks)
  - Use AES instead of RC4 for encryption
- *WPA2 certification has become mandatory for all new equipment certified by the Wi-Fi Alliance, ensuring that any reasonably modern hardware will support both WPA1 and WPA2.*

Wireless Attacks

- New wireless networks attacks have been created to target these networks
- These attacks include
  1. Rogue access points
  2. War Driving
  3. Bluesnarfing
  4. Blue Jacking

Rogue Access Point

A wireless AP is ROGUE if it fulfils the following criteria :

1. Connected to your secure wired network
   - thus broadcasting a signal someone can connect to potentially allowing access to your network and your resources. And
2. Controlled or managed by someone other than you
   - meaning you don't control the configuration, set up, encryption and authentication of users on that device.

Rogue Access Points

- An attacker who gained access the secure internal network via a rogue access point can directly attack all devices on the network.
- Bypass all of the network security and opens the entire network and all users to direct attacks

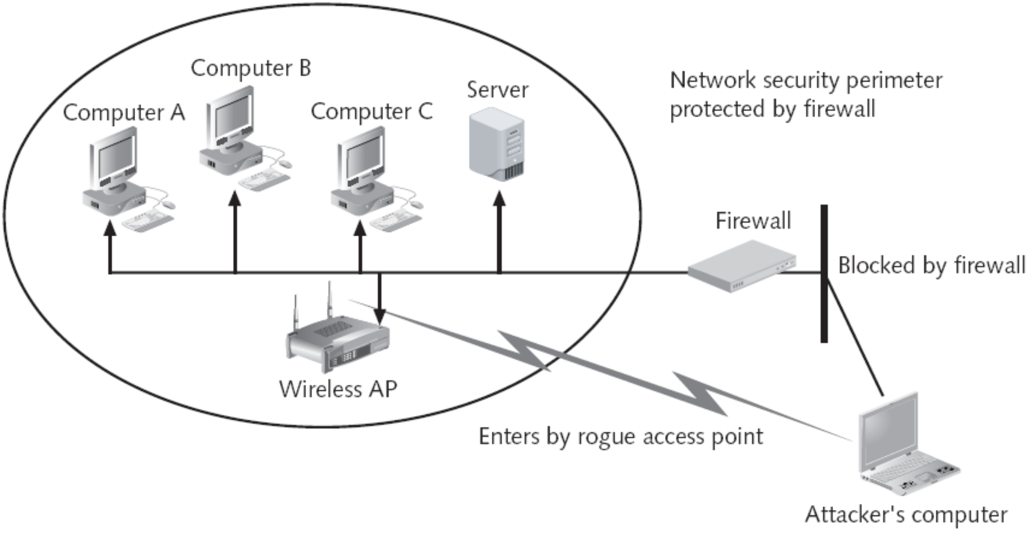


Figure 4-13 Rogue access point

War driving

- War driving technically involves using an automobile to search for wireless signals over a large area
  - At regular intervals, a wireless AP sends a beacon frame to announce its presence and to provide the necessary information for devices that want to join the network (Beaconing)
  - Each wireless device looks for those beacon frames (scanning)
  - Unapproved wireless devices can likewise pick up the beaconing RF transmission
  - Wardrivers are only out to log and collect information about the wireless access points (WAPs) they find while driving, without using the networks' services.
  - Example: CommView & AirCrack Video

War driving

- Softwares
  - AirCrack
  - AirSnort
  - Kismet
  - Cain & Able
  - WireShark
  - Fern WiFi Wireless Cracker

Cracking the Wifi AP

- Fluxion - a rewritten attack to trick inexperienced users into divulging the password/passphrase of the network.
- It jams the original network and creates a clone with the same name, enticing the disconnected user to join.
- The tool uses a captured handshake to check the password entered and continues to jam the target AP until the correct password is entered.
- https://www.youtube.com/watch?v=xzv5Vy9ghrg

Attack on Wireless Network

- **‘KRACK’ (**Key Reinstallation AttaCK) **WiFi Security Weakness**
  - *allows anyone to break WPA2 and steal data flowing between your wireless device and the targeted Wi-Fi network, such as passwords, chat messages and photos.*
- The weaknesses are in the Wi-Fi standard itself, and not in individual products or implementations.
- https://krebsonsecurity.com/2017/10/what-you-should-know-about-the-krack-wifi-security-weakness/

Bluesnarfing

- The unauthorized access of information from a wireless device through a Bluetooth connection
- Bluesnarfing involves the stealing of information from the victim's Bluetooth device.
- Due to vulnerability in vendor’s software and Bluetooth device set to discoverable.
- Allows an attacker to access e-mails, calendars, contact lists, and cell phone pictures and videos
  - By simply connecting to that Bluetooth device without the owner’s knowledge or permission

Blue jacking

- Sending unsolicited messages from Bluetooth to Bluetooth-enabled devices.
  - No mobile carrier required!
- Allows phone users to send business card anonymously using Bluetooth wireless technology.
- Usually harmless, annoying (like doorbell ditching) and no data is stolen.
- Avoid blue jacking by setting your bluetooth to non-discoverable.

Intrusion Detection Systems

Intrusion Detection System

(Preventive Measures)

- Firewall – A perimeter defence to block unauthorized access while permitting authorized communications.
- Example - security personnel at the gate

(Detection)

- (IDS) detects and report intrusion attempts to the network.
- Example - a security camera after the gate.

Intrusion Detection and Prevention System (IDPS) can block connections if it finds the connections is an intrusion attempt.

Intrusion Detection Systems

- The purpose of an intrusion detection system is to:
  - Identify **suspicious or malicious** activity.
  - Note activity that **deviates** from normal behavior.
  - **Catalog and classify** the activity.
  - **Respond** to the activity.
  - **Alert** Intrusion Attempts

- Intrusion detection systems are typically divided into **two main categories**, depending on how they monitor activity:
  - host-based (HIDS)
  - network-based (NIDS)

Host-Based IDS

- A host-based IDS is concerned only with activity on an individual system and usually has no visibility into the activity on the network or systems around it.
- It The HIDS looks for hostile, suspicious or malicious activities, such as:
  - *Logins at odd hours*
  - *Login authentication failures*
  - *Adding new user accounts*
  - *Modification or access of critical system files*
  - *Modification or removal of binary files (executables)*
  - *Starting or stopping processes*
  - *Privilege escalation*
  - *Using certain programs*
- It analyses operating system log files, looking for changes to system files and software, as well as network connections made by the host.
- *E.g alienvault, Norton Internet Security, Anti-virus etc*

Host-Based IDS

- The strength of host-based IDSs include:
  - Operating system-specific.
  - Application specific.
  - Examination of data after decryption.
  - Reduced false positive rates.
- disadvantages of HIDS:
  - a process on every system watched.
  - high cost of ownership.
  - uses local system resources.
  - difficult to maintain in large networks with different operating systems and configurations
  - has a focused view and cannot relate to activity around it.
  - can be disabled by attackers after the system is compromised.

Passive vs Active Host IDS

- Intrusion detection systems can be distinguished by
  - how they examine the activity around them and
  - whether or not they interact with that activity.
- A passive system **watches the activity, analyzes it, and generates alarms**.
  - It does not interact with the activity itself in any way.
  - It does not modify the defensive posture of the system to react to the traffic.
- An active IDS contains the same components and capabilities of passive IDS plus it **reacts to the activity** it is analyzing.
  - For example, it can send a TCP reset message to interrupt a potential attack.

Network-Based IDS

- A network-based IDS has visibility only into the traffic crossing the network link it is monitoring and typically has no idea of what is happening on individual systems.
- A network IDS (NIDS) examines network traffic as it passes by.
  - Bits and bytes traveling through cables interconnecting the systems.
  - It analyzes traffic by protocol, type, amount, source, destination, content, and traffic already seen.
  - The analysis happens quickly.
    - The IDS must be able to handle traffic at whatever speed the network operates to be effective.

Network-Based IDS

- What does it look for?
  - Like host-based systems, a network-based IDS looks for activities that represent **hostile actions or misuse**.
    - Denial-of-Service attacks
    - Port scans or sweeps
    - Malicious content in the data payload of a packet or packets
    - Vulnerability scanning
    - Trojans, viruses, or worms
    - Tunneling
    - Brute-force attacks

Network-Based IDS

- Advantages
  - It takes fewer systems to provide IDS coverage.
  - Deployment, maintenance, and upgrade costs are usually lower.
  - A network-based IDS has visibility into all network traffic and can correlate attacks among multiple systems.

- Disadvantages
  - It is ineffective when traffic is encrypted.
  - It cannot see traffic that does not cross it.
  - It must be able to handle high volumes of traffic.
  - It does not know about activity on the hosts themselves.

Active vs. Passive NIDS

- In a passive **NIDS** (Similar to HIDS)
  - it watches the traffic, analyzes it, and generates alarms. However, it does not interact with the traffic itself in any way or modify the defensive posture of the system to react to the traffic.

- An active NIDS contains all the same components and capabilities of the passive NIDS and may react to the traffic it is analyzing.

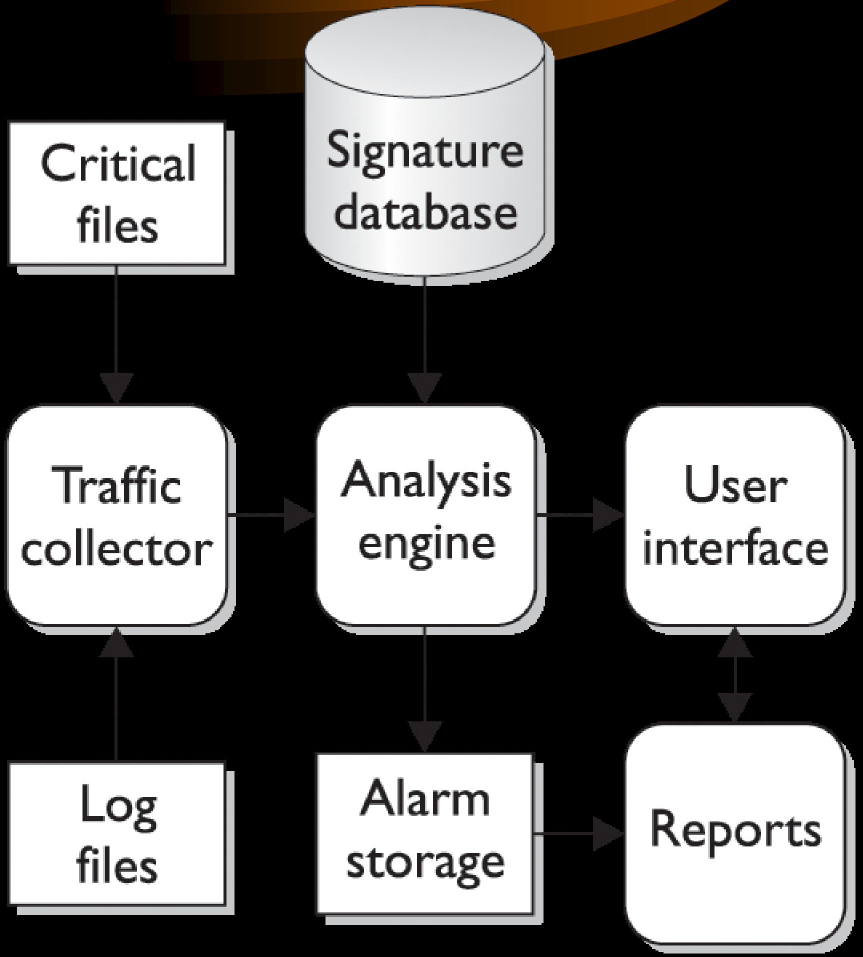
  2 types of Active NIDS :
  - Signature-based
  - Anomaly-based

Active vs. Passive NIDS

- Active NIDS
  - Signature-based
    - references a database of previous attack signatures
    - Each intrusion leaves a footprint behind (e.g., failed logins, file and folder access etc.).
    - These footprints are called signatures and can be used to identify and prevent the same attacks in the future.
    - Disadvantages : Signature database must be continually updated and maintained and Signature-based Intrusion Detection Systems (IDS) may fail to identify a unique attacks.
  - Anomaly-based
    - references a baseline or learned pattern of normal system activity to identify active intrusion attempts.
    - Deviations from this baseline or pattern cause an alarm to be triggered.
    - Disadvantages : Higher false alarms

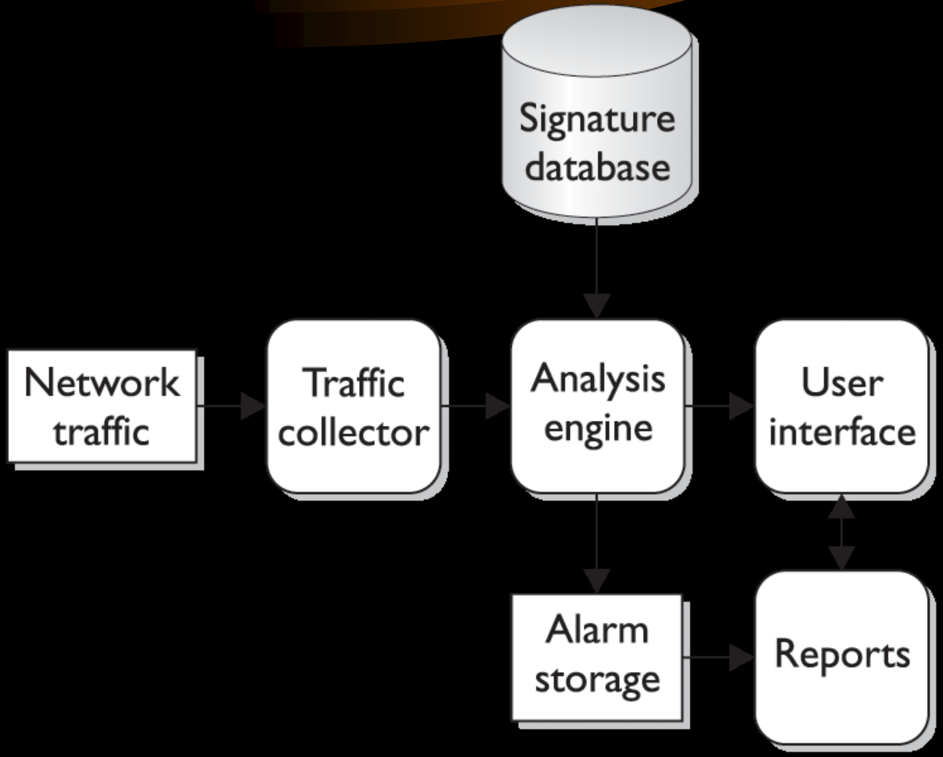
Host IDS Components

- Most HIDS focus on log files and audit trails generated by local operating systems.
  - Host-based systems use local system resources to operate.
  - Real time, looking for activity as it occurs.
  - Batch mode, looking for activity on a periodic basis.
  - They may be self-contained, but many of the newer commercial products have been designed to report to and be managed by a central system.



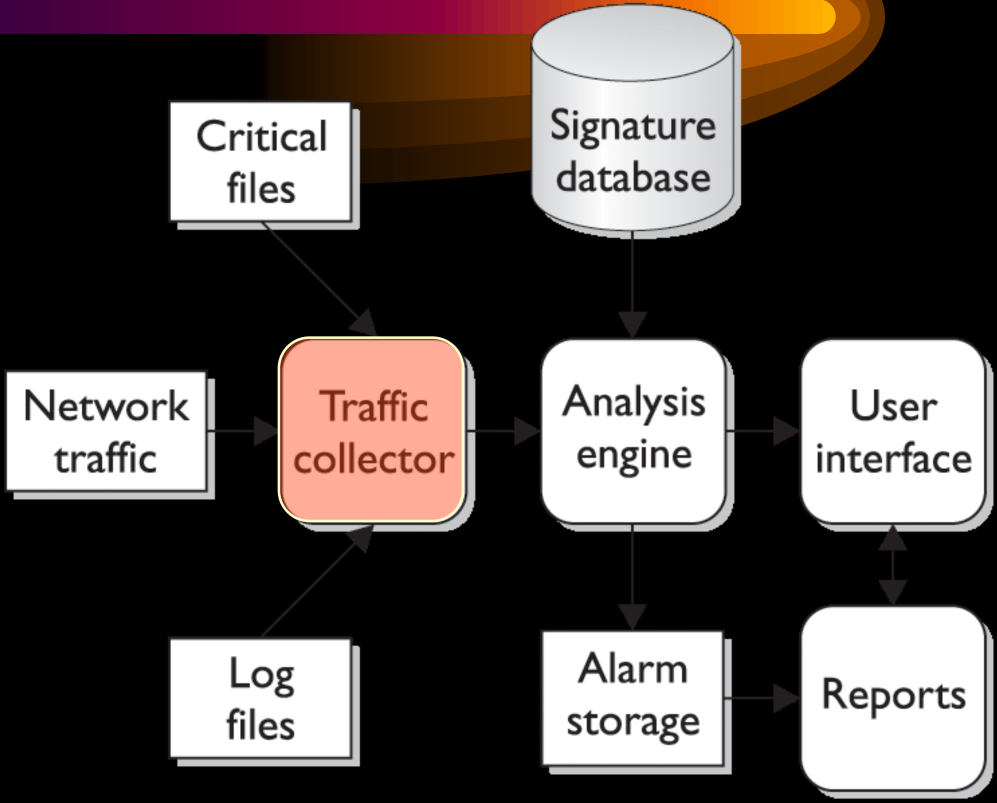
Network IDS Components

- Most NIDS focuses on network traffic.
  - Bits and bytes traveling through cables interconnecting the systems.
  - A network IDS (NIDS) examines network traffic as it passes by.
  - It must be able to analyze traffic by protocol, type, amount, source, destination, content, and traffic already seen.
  - The analysis must happen quickly.
  - The IDS must be able to handle traffic at whatever speed the network operates to be effective.



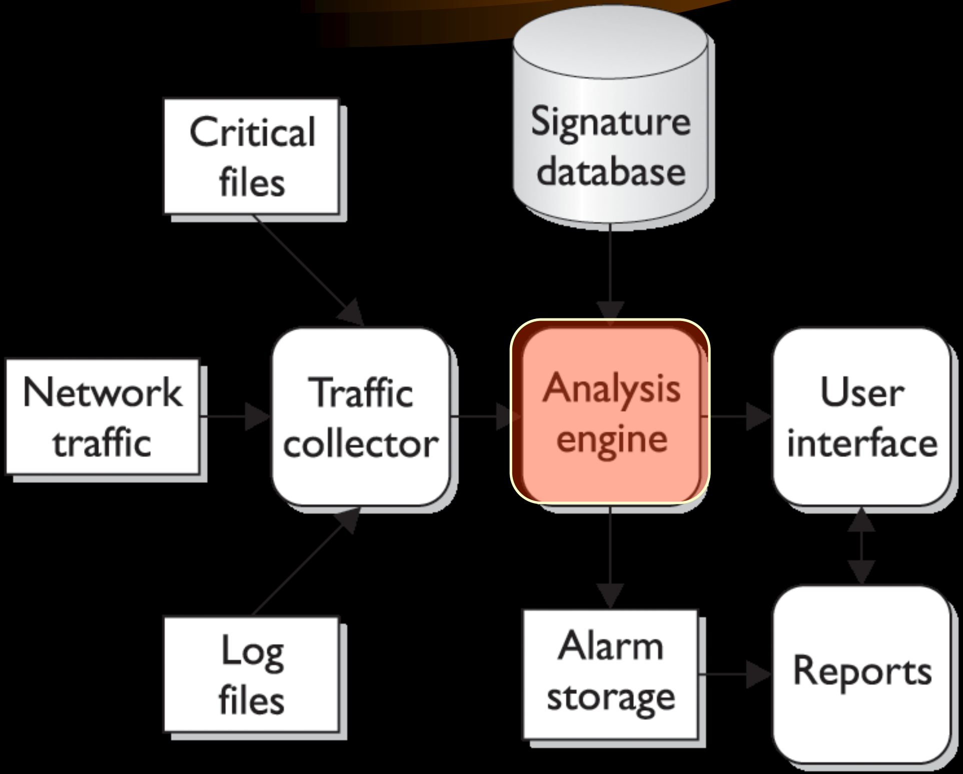
IDS Components

- **Traffic collector** collects activities/events for the IDS to examine.
  - On a host-based IDS, this could be log files, audit logs, or traffic coming to or leaving a specific system.
  - On a network-based IDS, this is typically a mechanism for copying traffic off the network link—basically functioning as a sniffer.



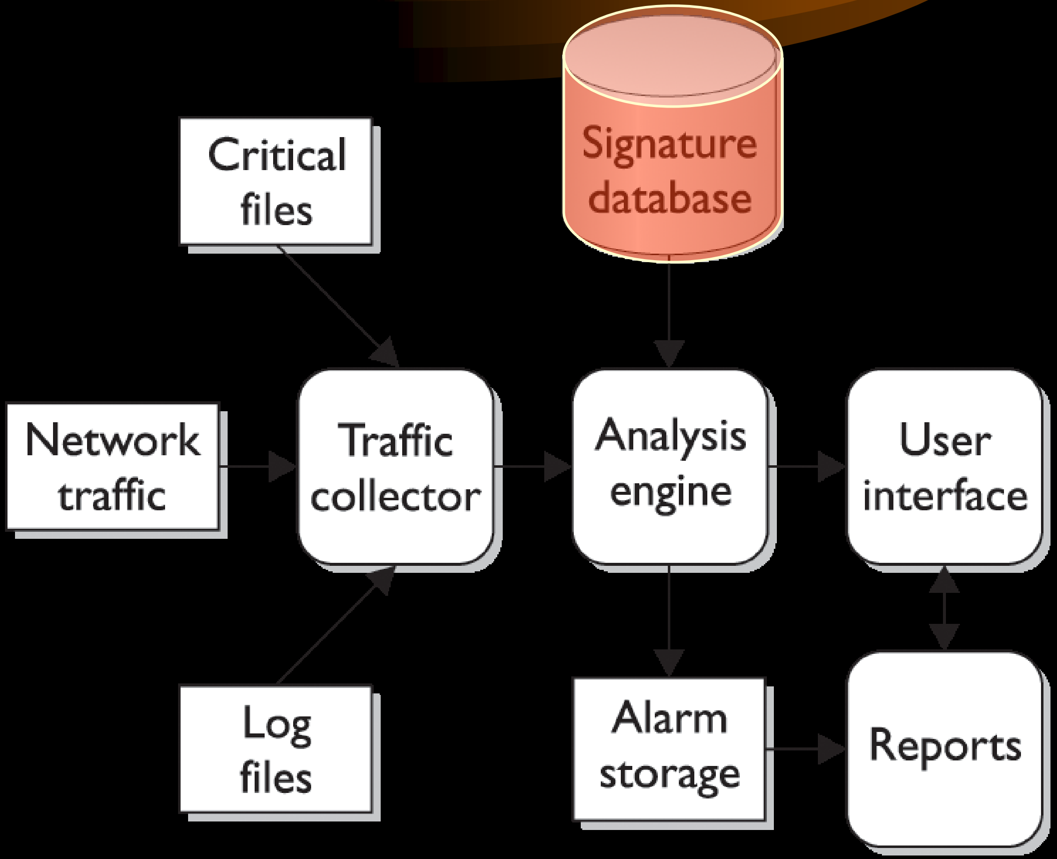
IDS Components

- **Analysis engine**:
  - Examines the collected network traffic and compares it to known patterns of suspicious or malicious activity stored in the signature database.



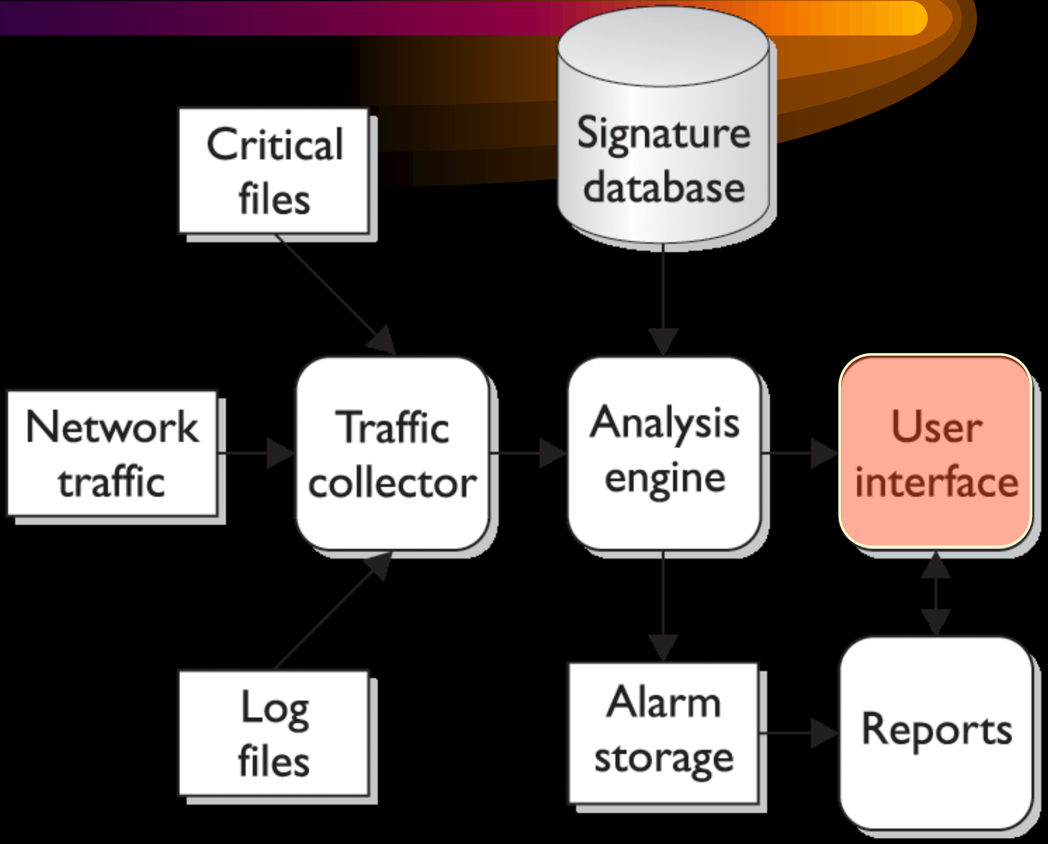
IDS Components

- **Signature database**:
  - Is a collection of patterns and definitions of known suspicious or malicious activity.



IDS Components

- **User interface and reporting:**
  - Is the component that interfaces with the human element, providing alerts when appropriate and giving the user a means to interact with and operate the IDS.



Tuning an IDS

- Most IDSs can be “tuned” to fit a particular environment.
  - Signatures may be turned off – the IDS will not look for certain types of traffic.
  - Alarm levels can be adjusted depending upon certain types of traffic.
  - Some IDS also allow users to “exclude” certain **patterns** of activity from specific hosts.