isep

École d'ingénieurs du numérique

Network Security

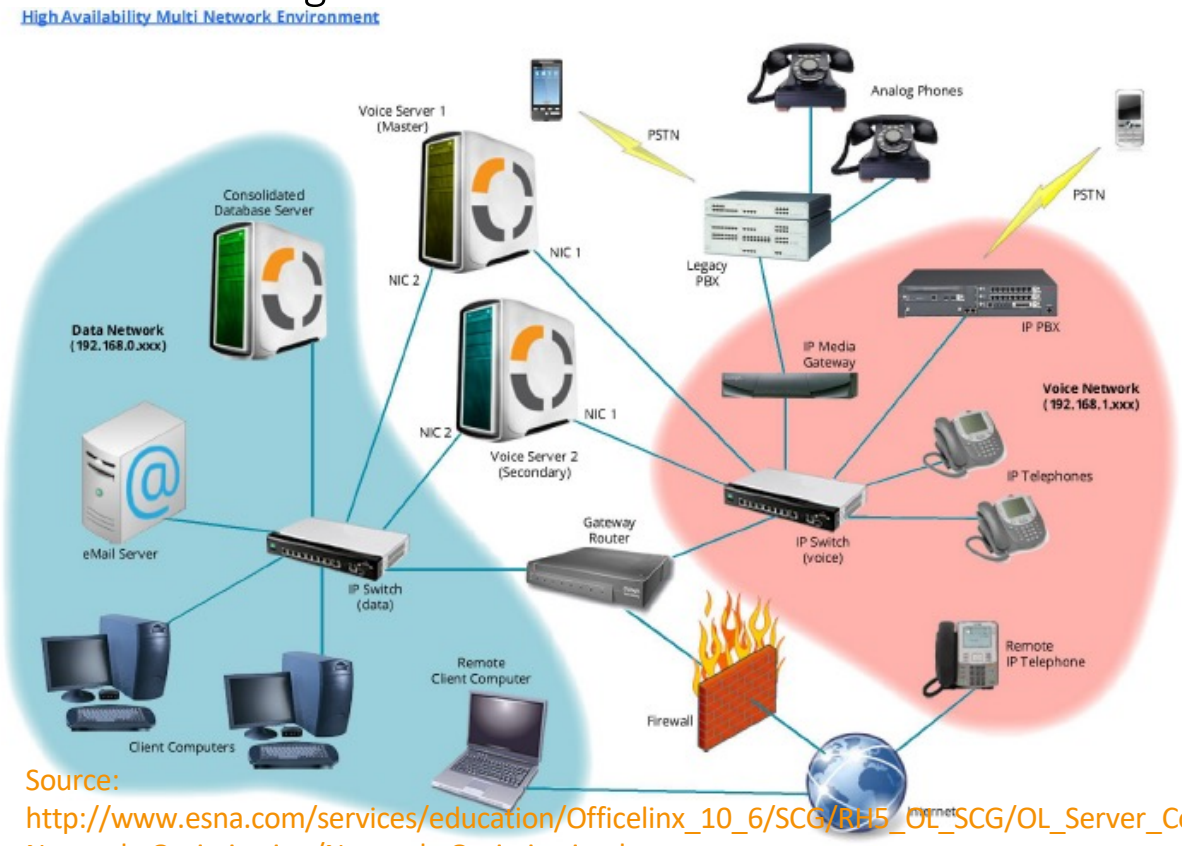
Secure Network Architecture and Securing Network Components

Nouredine TAMANI – nouredine.tamani@isep.fr

Cybersecurity – II.2317 Lecture #2 – 16/10/2023

Network Environment (1/2)

- Computers and networks emerge from the integration of:
  - communication devices,
  - storage devices,
  - processing devices,
  - security devices,
  - input devices,
  - output devices,
  - operating systems,
  - software,
  - services,
  - data,
  - and people.



Source: http://www.esna.com/services/education/Officelinx_10_6/SCG/R15_OL_SCG/OL_Server_Config_Network_Optimization/Network_Optimization.htm

Network Environment (2/2)

- An intranet is a private network that is designed to host the same information services found on the internet:
  - Access to the web, email, storage, etc. on internal servers that are not accessible outside the private network
  - If a networks relies on external entities to provide services internally then it is not considered intranets
- An extranet is a cross between the internet and an intranet:
  - It acts as an intranet for the private network
  - It can also serve information to internet via a section called a demilitarized zone (DMZ) or perimeter network
  - It is rarely on a public network

Outline

1. Can we trust the network?
2. Security within the network
3. Wireless network specificities
4. Collaboration tools and environments
5. Virtualization
6. Intrusion Detection Systems

1. Can we trust the network?

Introduction: Risk, Threat, Vulnerabilities

Security in the network (1/2)

It is not sufficient to protect the resources themselves (servers, applications...)

- Is our knowledge about network components and resources inventory up to date?
- Difficult to secure and keep secured all components involved in data processing for the company
  - Difficult to be sure that the proper security level is settled on the whole resources
- The geographical borders of the company are no more enough precise
- Internal and external notions are often impossible to define
  - The IS company perimetrical security is no more sufficient
  - This perimeter is very difficult to define: IS components may be geographically scattered
  - Defend a perimeter is not sufficient
  - Borders are unpredictable (new subsidiary purchase, externalization, cloud computing ...)
  - So, it is difficult to settle a homogeneous security

Security in the network (2/2)

- Necessity to partition the network to confine the risks
- Networks interconnection with various security policies
  - Various zones with different sensitivity inside the same company
  - Legacy, Office processing, Intranet, Internet web application
  - Research and development, Tests and qualification, Production, Backup
  - Accountability, Mailing, Browsing,...
- Services and information to put under more or less risks : public, half-public, private DMZ

IS security / Network security

The whole means of security must be homogeneous

- Aim of information security is to secure the IS and the company's set of assets:
- Means to achieve this aim must be coherently secured:
  - Example: a server can be logically well protected from network unauthorized accesses, but it is physically easy to access to

Network is just an angle to consider for security

- Security must be applied to all the links of the chain:
  - "Security is a chain whose weakest link characterize the resulting security level"
  - Security must be applied during information carrying level as well as during information storage, processing, archiving …
- This needs a coherent set of rules, physical, logical measures and procedures.
- **The only way to obtain this consistency is to define and deploy a Security Policy**

Various kind of attacks

- Active attacks:
  - Paralysis, Denial of Service, Saturation
  - Disguising (simulates connection process, IP or identity usurpation...)
  - Service hijacking
  - Alter information
- Passive attacks:
  - Screenshot
  - Unauthorized traffics listening
  - Routing modification
  - Radio emission capture
- Indirect attacks:
  - Asking for information through mailing

The 4 steps of today's strategy attack

TABLE 1 Listing of the 4 steps of today strategy attack

Infection	Persistence	Communication	Command & Control
Phishing (social engineering)	Rootkit	Encryption (SSL, SSH, etc.)	Command application
Hide transmission (SSL, P2P, etc.)	Backdoor	Proxy, Application tunnel	Update configure files
Remote exploit (shell access)	Anti-antivirus	Port evasion (tunnel over open ports)	EXE updates
Malware delivery (drive-by-download)		Fast flux (dynamic DNS)	Backdoor & proxy

Source https://www.paloaltonetworks.com

Modern attack strategy: Infection

- Getting user clicking on a bad link
  - Phishing mail, social networking site, sending him to an infected web page...
- Exploit runs
  - Infect with malware, buffer overflow, gaining shell access
- Deliver the malware in the background through application or connection already open
  - Drive-by-download
- Infection relies on hiding from evading security solutions
- Hide transmission so that security mechanisms can’t see the malware (SSL ...)
- A link is all that is required

Modern attack strategy: Persistence

- Maintain the bot on the compromised component
- Rootkit malware providing root-level (privileged) access to the compromised system
- Backdoor enables attacker to gain access to the system
- Anti anti-virus disables antivirus preventing detection of malware
  - Infecting the Master Boot Record (MBR)

Modern attack strategy: Communication

- Installed malware must be able
  - To communicate with the command & control components
  - To send extracted stolen data from the target
- Such communication must be stealthy, raising no suspicion
- It can be done through:
  - Encryption: SSL, SSH, proprietary encryption BitTorrent ...
  - Bypass, circumvention: using proxies, tunneling application within an allowed other one or an allowed protocol
  - Port evasion: via network anonymizer, tunnel over open port.
  - Botnet sends Command & Control (C&C) instructions through IRC...
  - Dynamic DNS: proxy traffic through multiple infected hosts, reroute it, making forensic difficult

Modern attack strategy: Command & Control

- Makes the malware or attack:
  - Controllable, manageable,
  - Up dateable: gives the attacker the ability to mutate and to be adapted to the weaknesses of the target
- Done through common applications:
  - Webmail, P2P network, social media, blog
  - Often encrypted, use backdoors and proxies
- Attacker goals:
  - How to infect, persist, communicate, control, update without being detected

2. Security within the network

OSI and TCP/IP Models

Attacks on Application Protocols: ICMP, ARP, DNS vulnerabilities

Risks and attacks of communication protocols

Main attacks on communication protocols: DOS/DDOS, Eavesdropping, Impersonation, Replay, Modification

Reminder: OSI Model

- A protocol is a set of rules and restrictions that define how data is transmitted over a network medium
- The International Organization for Standardization (ISO) developed the Open Systems Interconnection (OSI) Reference Model for protocols in the early 1980s
- Specifically, ISO 7498 defines the OSI Reference Model (called the OSI model).
- **The basis of secure network architecture and design is a thorough knowledge of the OSI model, TCP/IP model, and Internet Protocol (IP) networking in general**

Reminder: OSI Model

- The OSI model wasn't the first networking protocols or establish a common communications standard
- TCP/IP (based on the DARPA model, aka TCP/IP model), was developed in the early 1970s
- The OSI model is built upon 7 layers as illustrated in Figure 1.

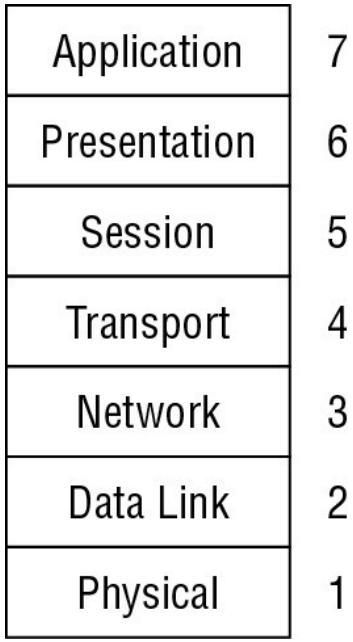


FIGURE 1 Representation of the OSI model

Reminder: OSI Model – Encapsulation / De-encapsulation

- Encapsulation is the addition of a header, and possibly a footer, to the data
- The previous layer's header and payload combine to become the payload of the current layer
- Encapsulation occurs from Application to Physical layers
- The inverse action from Physical to Application layers is de-encapsulation

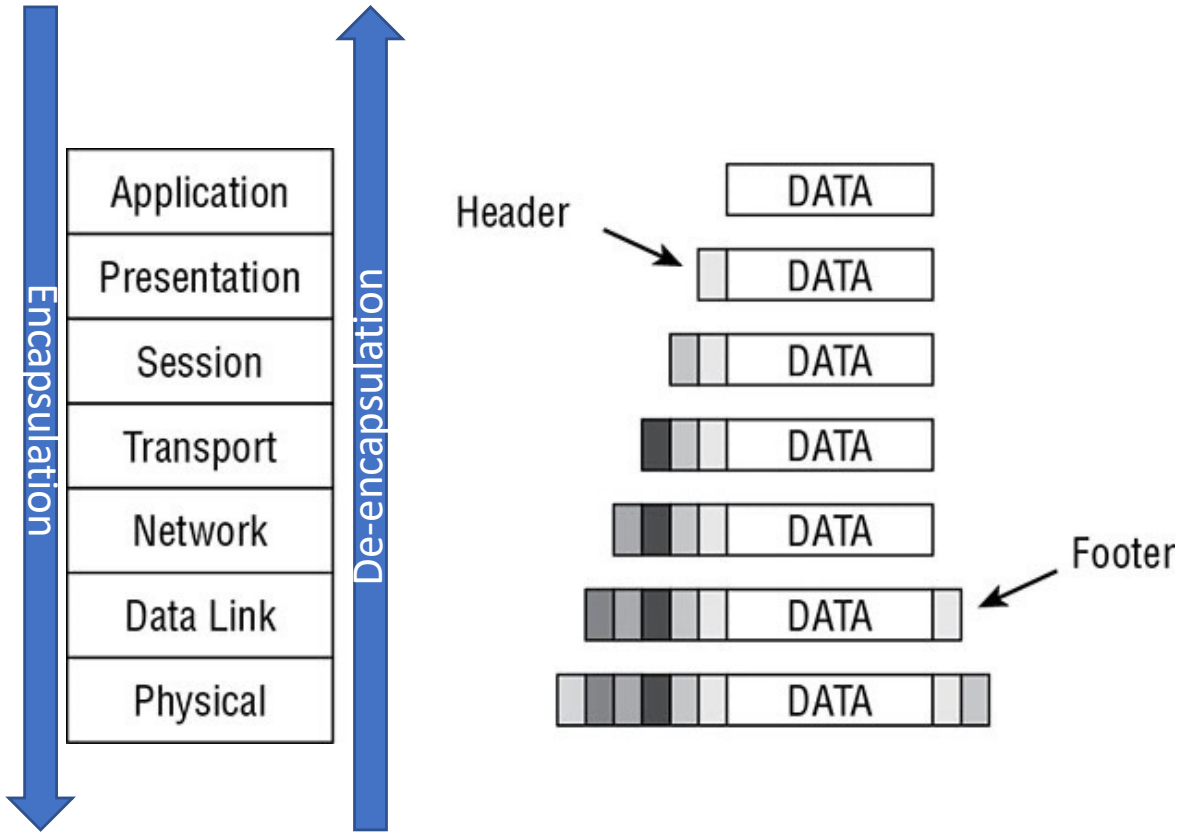


FIGURE 2 Representation of OSI model encapsulation/de-encapsulation

OSI Model: Data Names

Application	Data stream
Presentation	Data stream
Session	Data stream
Transport	Segment (TCP)/Datagram (UDP)
Network	Packet
Data Link	Frame
Physical	Bits

FIGURE 3 OSI model data names

- The message sent into the protocol stack at the Application layer is called the data stream
- In the Transport layer, data is called segment (TCP) or datagram (UDP)
- In the Network layer, it is called a packet
- In the Data Link layer, it is called a frame
- In the Physical layer, the data is converted into bits for transmission over the physical medium

TCP/IP Model

- TCP/IP model (DARPA or DOD model) consists of 4 layers:
  - Application (Process),
  - Transport (Host-to-Host),
  - Internet (Internetworking),
  - Link (Network Interface, or Network Access).
- The designers of the OSI Model took care to ensure that TCP/IP protocol suite fit their model.

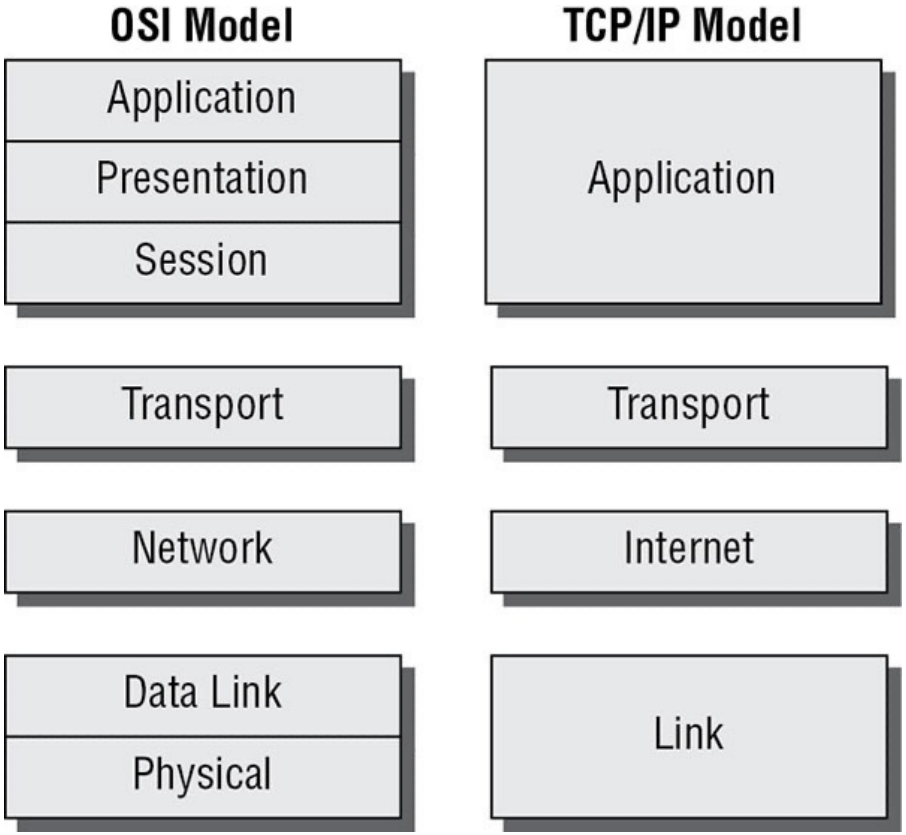


FIGURE 4 Comparing the OSI model with the TCP/IP model

TCP/IP Protocols

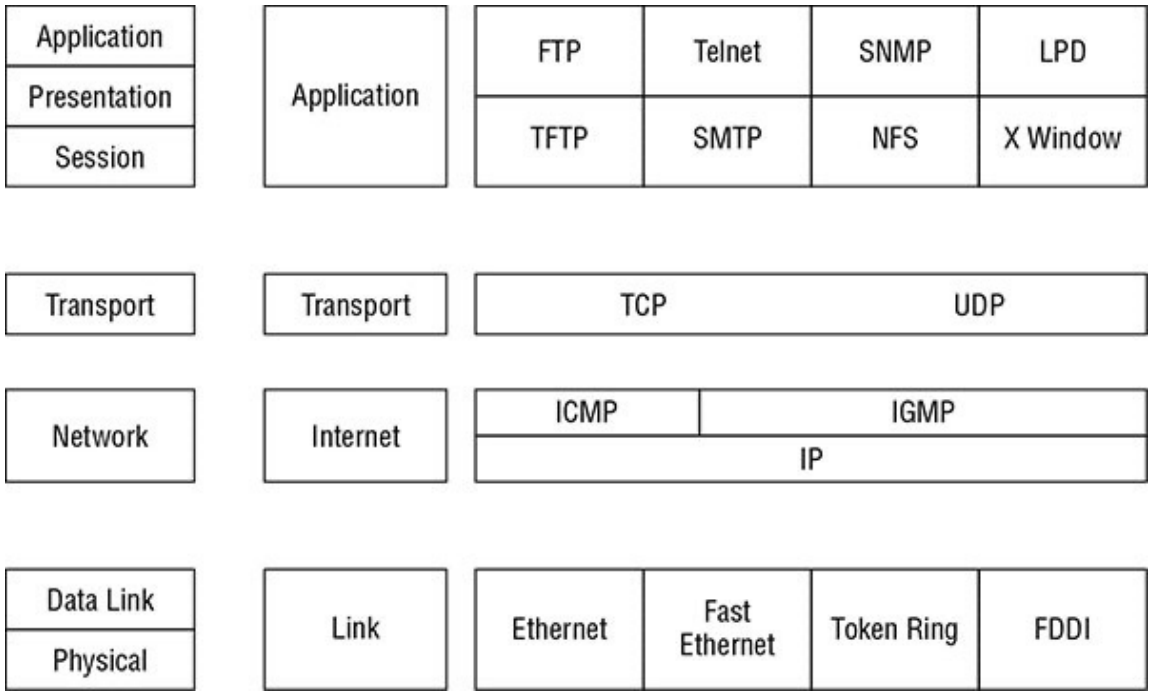


FIGURE 5 The four layers of TCP/IP and its component protocols

- TCP/IP can be found in just about every available operating system
- It consumes a significant amount of resources
- It is relatively easy to hack into because it was designed for ease of use rather than for security

Example: TCP/IP wireshark data

- en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
- options=6463<RXCSUM,TXCSUM,TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
- ether a4:83:e7:30:a8:33
- inet6 fe80::1c66:3b9e:2b2d:1546%en0 prefixlen 64 secured scopeid 0x6
- inet 172.24.5.244 netmask 0xfffff000 broadcast 172.24.15.255
- nd6 options=201<PERFORMNUD,DAD>
- media: autoselect
- status: active

Transport Layer Protocols: TCP and UDP

- Transmission Control Protocol (TCP) is a full-duplex connection-oriented protocol
- User Datagram Protocol (UDP) is a simplex connectionless protocol
- When a communication connection is established between two systems, it is done using ports
  - TCP and UDP each have 2^16 = 65,536 ports, since port numbers are 16-digit binary numbers
- A port allows a single IP address to be able to support multiple simultaneous communications
- The combination of an IP address and a port number is known as a socket

TCP channel establishment

- Transmission Control Protocol (TCP) operates at Transport layer:
  - It supports full-duplex communications,
  - It is connection oriented,
  - It employs reliable sessions.
- TCP is connection oriented: Handshake process (Figure 6)
  - The client sends a SYN flagged packet to the server
  - The server responds with a SYN/ACK flagged packet back to the client
  - The client responds with an ACK flagged packet back to the server

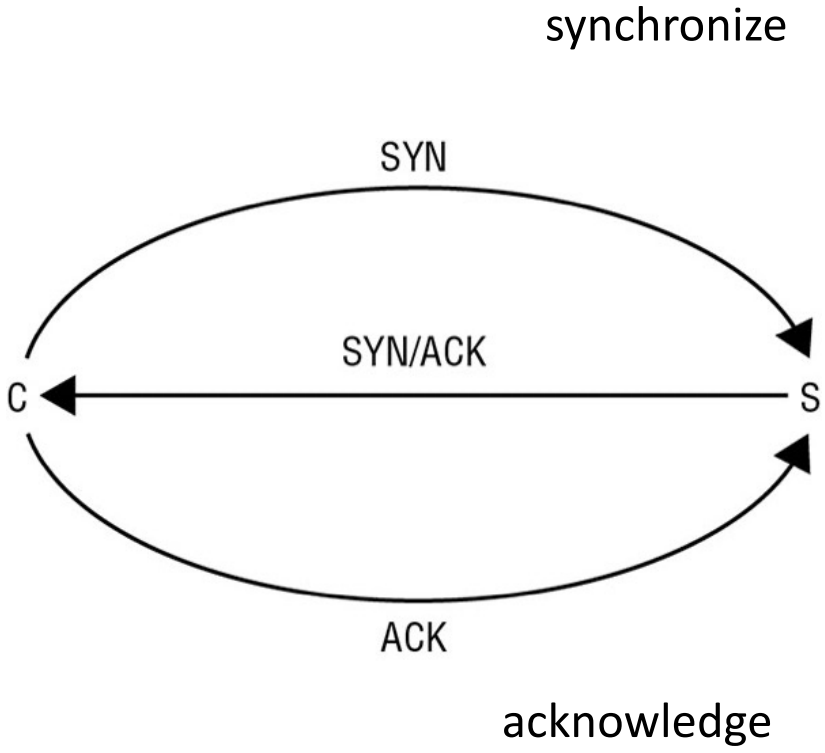


FIGURE 6 The TCP three-way handshake

TCP channel ending (2 methods)

- FIN (finish) flagged packets instead of SYN flagged packets:
  - Each side of a conversation will transmit a FIN flagged packet once all its data is transmitted,
  - triggering the opposing side to confirm with an ACK flagged packet,
  - It takes four packets to gracefully tear down a TCP session.
- RST (reset) flagged packet, which causes an immediate and abrupt session termination

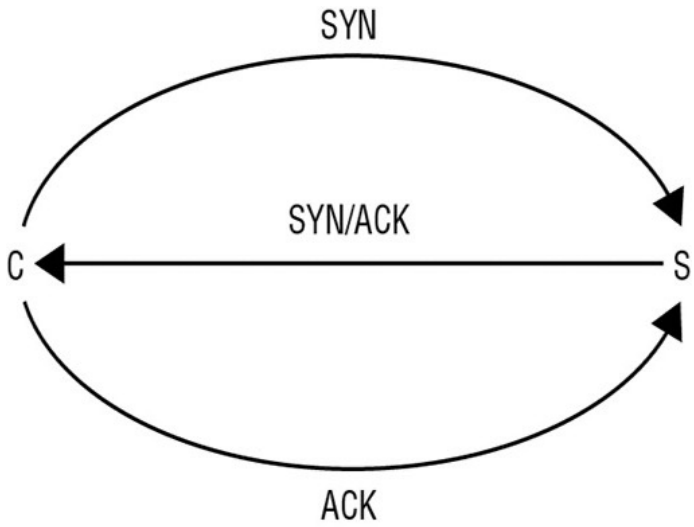


FIGURE 6 The TCP three-way handshake

Slowloris/HOIC (High Orbit Ion Cannon) attack

- It saturates the connection pool of a server with uncompleted TCP/IP channel establishment sequences
- Slowloris starts by making a full TCP connection to the remote server
- The tool holds the connection open by sending valid, **incomplete** HTTP requests to the server at regular intervals to keep the sockets from closing
- Since any Web server has limited resources, it will only be a matter of time before all sockets are used up and no other connection can be made
- HOIC is another famous application which can launch DoS attacks against websites

Source: https://www.unb.ca/cic/datasets/ids-2018.html

TCP/IP Protocol Discovery

- Hundreds of protocols are in use on a typical TCP/IP network at any given moment
- Using a sniffer, you can discover what protocols are in use on your current network
- Before using a sniffer, make sure you have the proper permission or authorization
- Download and install a sniffer, such as Wireshark:
  - Use the sniffer to monitor the activity on your network
  - Discover just how many protocols (subprotocols of TCP/IP) are in use on your network
  - Analyse the contents of captured packets
  - Pick out a few different protocol packets and inspect their headers:
  - Look for TCP, ICMP, ARP, and UDP packets.

Network Layer Protocols and IP Networking Basics

Internet Protocol (IP):

- IP provides route addressing for data packets
- It provides a means of identity and prescribes transmission paths
- Like UDP, IP is connectionless and is an unreliable datagram service
- IP does not offer guarantees that:
  - packets will be delivered,
  - packets will be delivered in the correct order,
  - packets will be delivered only once.
- You must employ TCP on IP to gain reliable and controlled communication sessions

TCP/IP Vulnerabilities

- Improperly implemented TCP/IP stacks are vulnerable to:
  - Buffer overflows, SYN flood attacks, DoS attacks, fragment attacks, oversized packet attacks, spoofing attacks, man-in-the-middle attacks, hijack attacks, and coding error attacks.
- TCP/IP is also subject to passive attacks via monitoring or sniffing:
  - Network monitoring is the act of monitoring traffic patterns to obtain information about a network
  - Packet sniffing is the act of capturing packets from the network in hopes of extracting useful information from the packet contents:
    - Usernames, passwords, email addresses, encryption keys, credit card numbers, IP addresses, system names, and so on.

Internet Control Message Protocol: ICMP

- ICMP is used to determine the health of a network or a specific link
- ICMP is utilized by ping, traceroute, pathping, and other network management tools
- The ping utility employs ICMP echo packets and bounces them off remote systems
- You can use ping to determine whether:
  - The remote system is online,
  - The remote system is responding promptly,
  - The intermediary systems are supporting communications,
  - The level of performance efficiency at which the intermediary systems are communicating.
- The ping utility includes a redirect function that allows the echo responses to be sent to a different destination than the system of origin

Internet Control Message Protocol (ICMP) – attacks

- ICMP is often exploited in various forms of bandwidth-based denial-of-service (DoS) attacks:
  - Ping of death sends a malformed ping larger than 65,535 bytes (maximum IPv4 packet size) to a computer to attempt to crash it
  - Smurf attacks generate enormous amounts of traffic on a target network by spoofing broadcast pings
  - Ping floods are a basic DoS attack relying on consuming all of the bandwidth that a target has available
- Many networks limit the use of ICMP or at least limit its throughput rates

Address Resolution Protocol (ARP)

- ARP is a subprotocol of the TCP/IP protocol suite and operates at the Data Link layer (layer 2)
- Resolve IP addresses (32-bit binary number) into Media Access Control (MAC) addresses (48-bit binary number)—or EUI-48 or even EUI-64
- Traffic on a network segment is directed from its source system to its destination system using MAC addresses
- ARP uses caching and broadcasting to perform its operations.
- The first step in resolving an IP address into a MAC address, or vice versa, is to check the local ARP cache

Address Resolution Protocol (ARP) - Attacks

ARP cache poisoning:

- In ARP cache poisoning an attacker inserts bogus information into the ARP cache
- It is a register of already resolved MAC Addresses
- If an address is not in the cache, the system will use its default gateway to transmit its communications
- Then, the default gateway (in other words, a router) will need to perform its own ARP process

ARP spoofing:

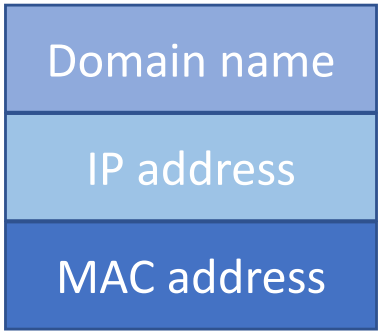
- ARP spoofing provides false MAC addresses for requested IP-addressed systems to redirect traffic to alternate destinations
- ARP attacks are often an element in man-in-the-middle attacks

Address Resolution Protocol (ARP) – countermeasures

- Defining static ARP mappings for critical systems
- Monitoring ARP caches for MAC-to-IP-address mappings
- Using an IDS to detect anomalies in system traffic and changes in ARP traffic

Domain Name Systems - DNS

- Addressing and naming make network communications possible:
  - It is much easier to remember google.com than 64.233.187.99
- There are three different layers to be aware of: (in reverse order)
  - MAC address: hardware address is a “permanent” physical address.
  - IP address: is a “temporary” logical address assigned over or onto the MAC address.
  - Domain name: computer name is a “temporary” human-friendly convention assigned over or onto the IP address.



Domain Name Systems - DNS

- To resolve a DNS name into an IP address, a computer:
  - Checks the local cache (which includes content from the HOSTS file)
  - Sends a DNS query to a known DNS server
  - Sends a broadcast query to any possible local subnet DNS server
- If the client doesn't obtain a DNS-to-IP resolution from any of these steps, the resolution fails, and the communication can't be sent

DNS Poisoning

- Attacks on DNS is called resolution attacks
- DNS poisoning is the act of falsifying the DNS information to reach a desired system
- The easiest way is to corrupt the HOSTS file or the DNS server query
- An attacker might use one of these techniques:
  - Deploy a rogue DNS server (aka DNS spoofing or DNS pharming)
  - Alter the HOSTS file
  - Corrupt the IP configuration
  - Use proxy falsification (used for web applications)

DNS Spoofing

- DNS spoofing occurs when an attacker sends false replies to a requesting system
- In 2008, a significant vulnerability was discovered and disclosed by Dan Kaminsky:
  - By sending falsified replies to a caching DNS server for non-existent subdomains, an attacker can hijack the entire domain's resolution details
  - For more details how DNS works and how this vulnerability threatens the current DNS infrastructure: http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

DNS Poisoning: some countermeasures

Some basic security measures that can reduce their threat:

- Allowing only authorized changes to DNS
- Logging all privileged DNS activity
- Limit zone transfers from internal DNS servers to external DNS servers:

  → Blocking inbound TCP port 53 (zone transfer requests) and UDP port 53 (queries)
- Limit the external DNS servers from which internal DNS servers pull zone transfers
- Deploy a network intrusion detection system (NIDS)
- Properly harden all DNS, server, and client systems in your private network
- Use DNSSEC to secure your DNS infrastructure
- Require internal clients to resolve all domain names through the internal DNS:

  → Blocking outbound UDP port 53 (for queries) while keeping open outbound TCP port 53 (for zone transfers)

DNS Pharming

- DNS pharming is related to DNS poisoning (by modifying the local HOSTS file) and/or DNS spoofing
- Pharming is the malicious redirection of a valid website's URL or IP address to a fake website (false version of the original valid site)
- This is often part of a phishing attack where the attacker is attempting to trick victims into giving up their logon credentials

Domain Hijacking

- Domain hijacking, or domain theft, is the malicious action of changing the registration of a domain name without the authorization of the valid owner
- This may be accomplished by stealing the owner's logon credentials
- Register a domain name immediately after the original owner's registration expires:
  - When it happens, no recourse other than to contact the new owner and inquire regarding reobtaining control
  - Many registrars have a "you snooze, you lose" policy for lapsed registrations
- Example of a domain hijack: the theft of the Fox-IT.com domain in Sep. 2017:
  - Read more at https://www.fox-it.com/en/insights/blogs/blog/fox-hit-cyber-attack/

DNS Homograph Attack

- Homograph attacks leverage similarities in character sets to register phony international domain names (IDNs) that appear legitimate to the naked eye
- For example, some letters in Cyrillic look like Latin characters:
  - Example: the **p** in Latin looks like the **p** (ER) Cyrillic letter.
  - So, domain names like apple.com or paypal.com might look valid as Latin characters but include Cyrillic characters
  - For a thorough discussion of the Homograph attack, see https://blog.malwarebytes.com/101/2017/10/out-of-character-homograph-attacks-explained/
- The only real solution is to upgrade DNS to Domain Name System Security Extensions (DNSSEC)

Threats against communication system

- Main attacks:
  - Denial of service (DOS, DDOS),
  - Eavesdropping,
  - Impersonation,
  - Replay,
  - Modification.

Denial-of-service attack: DoS and DDoS

- A DoS attack is a resource consumption attack:
  - →The goal is preventing legitimate activity on a victimized system
  - →The target is rendered unable to respond to legitimate traffic
- Two basic forms of denial of service:
  - Attacks exploiting a vulnerability in hardware or software:
    - Weakness, error, or standard feature of software to cause a system to hang, freeze, consume all system resources, etc.
  - Attacks that flood the victim's communication pipeline with garbage network traffic:
    - Traffic generation or flooding attacks
- Some attacks exploit specific protocols:
  - Internet Protocol (IP), Transmission Control Protocol (TCP), Internet Control Message Protocol (ICMP), and User Datagram Protocol (UDP)

Denial-of-service attack: DoS and DDoS

- Many DoS attacks begin by compromising or infiltrating one or more intermediary systems:
  - Used to hide the attacker from the victim
  - These intermediary systems are commonly referred to as secondary victims
  - The attacker installs remote-control tools, often called bots, zombies, or agents, onto these systems to turn them to an attack platform
- Distributed denial-of-service (DDOS): is an attack involving zombie systems
- Botnets: are deployments of numerous bots or zombies across numerous unsuspecting secondary victims

Denial-of-service attack: DoS and DDoS

Some countermeasures and safeguards against these attacks:

- Add firewalls, routers, and intrusion detection systems (IDSs) that:
  - Detect DoS traffic, automatically block ports, and filter out packets based on the source or destination address
- Maintain good contact with your service provider to request filtering services when a DoS occurs:
  - Disable echo replies on external systems
  - Disable broadcast features on border systems
  - Block spoofed packets from entering or leaving your network
- Keep all systems patched with the most security updates from vendors
- Despite the cost, consider commercial DoS protection/response services

Eavesdropping

- Eavesdropping is listening to communication traffic to duplicate it:
  - Recording data to a storage device
  - Using an extraction program that dynamically extracts the content from the traffic stream
  - Confidential contents such as usernames, passwords, process procedures, data, etc.
- Eavesdropping usually requires physical access to the IT infrastructure:
  - To connect a physical recording device to an open port or cable splice
  - To install a software-recording tool onto the system
- Eavesdropping is often facilitated using a network traffic capture or monitoring program or a protocol analyzer system (a sniffer)
- Eavesdropping is generally a passive attack but when it is used to alter or inject communications, it is said active attack

Eavesdropping: countermeasures

- Maintain physical access security to prevent unauthorized personnel from accessing your IT infrastructure
- Use encryption (IPsec or SSH) methods on communication traffic
- Exercise: you can see all the data that passes your network interface:
  - Sniffers: Wireshark and NetWitness
  - Dedicated eavesdropping tools: T-Sight, Zed Attack Proxy (ZAP), and Cain & Abel
  - You can experiment with a few eavesdropping tools only on networks for which you have the proper approval and authorization!!!!!!

Impersonation/Masquerading

- Impersonation, or masquerading: pretending to be someone or something you are not to gain unauthorized access to a system
  → Authentication credentials have been stolen or falsified to satisfy authentication mechanisms
- Impersonation is possible through the capture of usernames and passwords or of session setup procedures for network services
- Some solutions to prevent impersonation:
  - Onetime pads authentication
  - Token authentication systems, using Kerberos,
  - Encryption to increase the difficulty of extracting authentication credentials from network traffic

Replay Attacks, modifications Attacks

- Replay Attacks: an offshoot of impersonation attacks
  - Attempt to re-establish a communication session by replaying captured traffic against a system
  - Countermeasures: using onetime authentication mechanisms and sequenced session identification
- Modification Attacks
  - Captured packets are altered and played against a system to bypass the restrictions of improved authentication mechanisms and session sequencing
  - Countermeasures: using digital signature verifications and packet checksum verification

Hyperlink Spoofing

- Hyperlink spoofing is like DNS spoofing
  - Used to redirect traffic to a rogue or imposter system
- An alteration of the hyperlink URLs in the HTML code of documents sent to clients
- Are usually successful because most users assume that the hyperlink is valid and just click it
- Phishing is another attack that commonly involves hyperlink spoofing
- Phishing attacks can take many forms, including the use of false URLs

Hyperlink Spoofing: countermeasures

- Be wary of any URL or hyperlink in an email, PDF file, or productivity document
- If you want to visit a site offered as such:
  - Go to your web browser and manually type in the address,
  - Use your own preexisting URL bookmark,
  - Use a trusted search engine to find the site.
- These methods involve more work on the user part, but they will establish a pattern of safe behavior that will serve you well
- Keeping your system patched and using the internet with caution

Securing Wireless Networks

WIFI standards

Attacks on Wireless networks

There are also risks on Bluetooth, RFID, NFS, Cell phones.

Wireless Networks

- A wireless network is a network that uses wireless data connections between network nodes
  - Easy to deploy with a low cost
  - Devices can roam freely within the signal range of the network
- 802.11 is the IEEE standard for wireless network communications
- Various versions of the standard have been implemented:
  - 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac ➔ 802.11x
  - Each version of 802.11 standard offered a better throughput: 2 MB, 11 MB, 54 MB, 200 MB+, and 1 GB respectively
  - b, g, and n amendments all use the same frequency to maintain backward compatibility
  - Do not confuse with 802.1x: authentication technology

Securing Wireless Access Points (WAP)

- Wireless cells are the areas within a physical environment where a wireless device can connect to a WAP
- Adjusting the strength of the WAP to maximize authorized user access and minimize intruder access
- Historically, wireless networking has been insecure:
  - Lack of knowledge by end users and organizations
  - Insecure default configurations set by device manufacturers
- In addition to risks identified in wired networks, wireless networks are subject to distance eavesdropping, packet sniffing, and new forms of DoS and intrusion

Securing Wireless Access Points (WAP)

- Deploying wireless networks configured to use infrastructure mode rather than ad hoc mode:
  - Ad hoc mode means that any two wireless networking devices can communicate without a centralized control authority.
  - Infrastructure mode means that a WAP is required and the restrictions of the WAP for wireless network access are enforced.
- Several variations of the infrastructure mode:
  - Stand-alone,
  - Wired extension,
  - Enterprise extended,
  - Bridge.

Securing the Service Set IDentifier (SSID)

- Wireless networks are assigned a SSID (either Basic SSID or Extended SSID)
- If multiple base stations or WAPs are involved in the same wireless network, an extended station set identifier (ESSID) is defined
- Knowledge of the SSID does not always grant entry
- SSIDs are defined by default by vendors, and should be changed to something unique before deployment
- The SSID is broadcasted by the WAP via a beacon frame to allow any wireless NIC within range to see the wireless network
- Is disabling the default broadcasting of the SSID useful as security measures?
  - Attackers can still discover the SSID with a wireless sniffer

Using Secure Encryption Protocols

- The IEEE 802.11 standard defines 2 methods for a user to authenticate to WAPs:
  - Open system authentication (OSA)
  - Shared key authentication (SKA)
- OSA means there is no real authentication required:
  - Everything is transmitted in clear text (no secrecy or security)
- SKA means that authentication must take place before any communications:
  - The 802.11 standard defines Wired Equivalent Privacy (WEP) => WEP should not be used anymore
  - Later amendments to the original 802.11 standard added WPA, WPA2, WPA3 and other technologies

Wi-Fi Protected Access (WPA)

- WPA is an improvement over WEP:
  - It negotiates a unique key set with each host
  - However, a single passphrase is used to authorize the association with the base station
  - If the passphrase is not long enough, it could be guessed
  - Usually, 14 characters or more for the passphrase is recommended
- 802.11i is the amendment that defines a cryptographic solution to replace WEP
- When 802.11i was finalized, WPA solution was already widely used, so it was branded WPA2:
  - But this does not indicate that 802.11i is the second version of WPA
- 802.11i, or WPA2, implements concepts like IPSec

Wi-Fi Protected Access (WPA)

- WPA is based on:
  - Lightweight Extensible Authentication Protocol (LEAP) and Temporal Key Integrity Protocol (TKIP) and a secret passphrase for authentication
- Drawbacks of WPA:
  - The use of a single static passphrase
  - A brute-force guessing attack against a WPA network to discover the passphrase
  - Passphrase should be 14 characters or more, but it is not impossible to crack
  - both LEAP and TKIP encryption are now crackable

→ WPA no longer provides long-term reliable security and should not be used anymore

Wi-Fi Protected Access 2 and 3 (WPA2/WPA3)

- WPA2 is the amendment of 802.11i released in 2004 which implements CCMP:
  - CCMP: **Counter Mode Cipher Block Chaining Message Authentication Code Protocol**
  - AES: Advanced Encryption Standard
- In late 2017, a KRACK (Key Reinstallation AttaCKs) attack (https://www.krackattacks.com/) was disclosed
- WPA3 announced in 2018 to replace WPA2, it uses:
  - An equivalent 192-bit cryptographic strength in WPA3-Entreprise mode (AES-256 and SHA-384)
  - CCMP-128 as the minimum encryption algorithm in WPA3-Personal mode
- The WPA3 standard replaces the Pre-Shared Key exchange with Simultaneous Authentication of Equals as defined in IEEE 802.11-2016

802.1X/EAP

- Using 802.1X, other techniques and solutions can be integrated into wireless networks:
  - Remote Authentication Dial-In User Service (RADIUS)
  - Terminal Access Controller Access Control System (TACACS)
  - Certificates, smart cards, token devices, and biometrics

MAC Filter

- A MAC filter is a list of authorized wireless client interface MAC addresses, used by a WPA to block access to all nonauthorized devices
- It can be difficult to manage and tends to be used only in small, static environments:
  - Your own internet box at home or in small businesses for instance
- A hacker can discover the MAC address of a valid client and then spoof that address onto their attack wireless client

Wi-Fi Protected Setup (WPS)

- WPS simplifies adding new clients to a well-secured wireless network
- It operates by auto-connecting the first new wireless client to seek the network
- It also uses a code or personal identification number (PIN) to trigger WPS negotiation without the need to physically press the button:
  - It is possible to guess the WPS code in hours (~ 6h)
- WPS is enabled by default on most WAP as required by device Wi-Fi Alliance certification
  - It's important to disable it as part of a security-focused pre-deployment process
- If we need to add numerous clients to a network, temporarily reenable WPS:
  - Be sure to disable it immediately afterward

Using Captive Portals

- A captive portal is an authentication technique that redirects a newly connected wireless web client to a portal access control page
- The portal page can require the user to input payment information, provide logon credentials, or input an access code
- It displays an acceptable user policy, privacy policy, and tracking policy, and user consent to the policies before being able to communicate across the network
- Can be found in public areas, such as hotels, restaurants, bars, airports, libraries, etc.

General Wi-Fi Securing Procedure

Here are the steps (order does not imply which step offers more security):

- Change the default administrator password
- Decide whether to disable the SSID broadcast based on your deployment requirements
- Change the SSID to something unique
- Enable MAC filtering if the pool of wireless clients is relatively small (usually less than 20) and static
- Consider using static IP addresses
- Configure DHCP with reservations (applicable only for small deployments)
- Turn on the highest form of authentication and encryption supported, which is currently WPA2 or WPA3
- Treat wireless as remote access and manage access using 802.1X
- Treat wireless as external access and separate the WAP from the wired network using a firewall
- Treat wireless as an entry point for attackers and monitor all WAP-to-wired-network communications with an intrusion detection system (IDS)
- Require all transmissions between wireless clients and WAPs to be encrypted (VPN link)

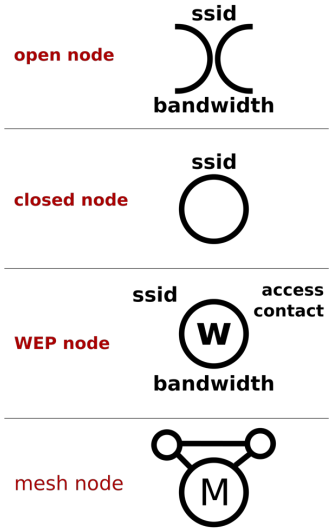
Wireless Attacks

- Security should be an end-to-end solution that addresses all forms, methods, and techniques of communication
- Some wireless specific attacks:
  - War driving
  - War chalking
  - Replay
  - Initialization Vector
  - Rogue Access Points
  - Evil twin

War Driving

- War driving is the act of using a detection tool to look for wireless networking signals
- The name comes from the legacy attack concept of war dialling:
  - To discover active computer modems by dialling all the numbers in a prefix or an area code
- War driving can be performed with:
  - Any device having wireless capabilities,
  - By using native features of the OS,
  - Using specialized scanning and detecting tools.

War Chalking



- War chalking is a type of geek graffiti that some wireless hackers used during the early years of wireless (1997–2002)
- War chalking was used to disclose to others the presence of a wireless network in order to share a discovered internet link
- Currently, the need for and occurrence of war chalking has faded. Why?

Replay

- Retransmission of captured communications in the hope of gaining access to the targeted system
- Many variants exist:
  - Capturing new connection requests of a client and then replaying it to fool the base station into responding as if another new client connection request was initiated
  - Focusing on DoS by retransmitting connection or resource requests to keep the base station busy
- Wireless replay attacks can be mitigated by:
  - Keeping the firmware of the base station updated
  - Operating a wireless-focused network intrusion detection system (NIDS)
  - A W-IDS or W-NIDS will be able to detect such abuses

Initialization Vector IV

- IV is a mathematical and cryptographic term for a random number
- IVs increase algorithm security by reducing predictability and repeatability
- IV is a point of weakness if it's too short, exchanged in plain text, or selected improperly
- An IV attack is an exploitation of how the IV is handled (or mishandled)
  - The WEP IV is only 24 bits long and is transmitted in plaintext
  - As WEP doesn't check for packet freshness, then it allows a live WEP crack to be successful in < 60s

Rogue Access Points

- A rogue WAP may be planted by an employee for convenience, or it may be operated externally by an attacker:
  - A wireless access point planted by an employee can be connected to any open network port
- Such unauthorized access points usually aren't configured for security or, if they are, aren't configured properly
- Rogue wireless access points should be discovered and removed
- 2 methods to attacking wireless clients:
  - Make clients with saved wireless profiles to inadvertently connect to the rogue WAP instead of the valid original WAP
  - Attract new visiting wireless clients
- The defense against rogue WAPs is:
  - To be aware of the correct and valid SSID
  - Operate a wireless IDS to monitor the wireless signals for abuses

Evil Twin

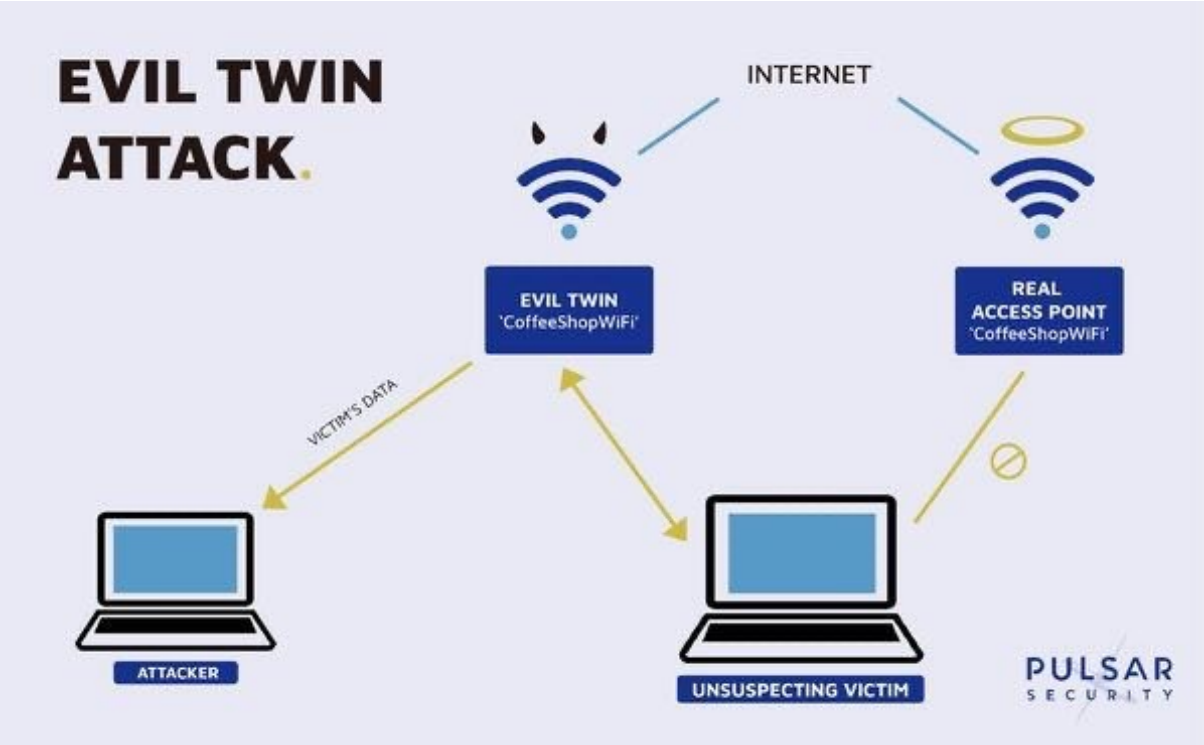


Figure 7 Evil Twin schematization.

Evil Twin

- Evil twin attack: a hacker operates a false access point that will automatically clone, or twin, the identity of an access point based on a client device's request to connect
- The evil twin attack system eavesdrops on the wireless signal for reconnect requests
- It spoofs their identity with those parameters and offers a plaintext connection to the client
- The client accepts the request and establishes a connection with the evil twin base station
- This enables the hacker to eavesdrop on communications through a man-in-the-middle attack:
  - Which could lead to session hijacking, data manipulation credential theft, and identity theft
- To defend against evil twin attacks:
  - Pay attention to the wireless network your devices connect to
  - Prune unnecessary and old wireless profiles from your history list to give attackers fewer options to target

Secure Network Components

Firewalls

Firewalls

- Firewalls are essential tools in managing, controlling and filtering network traffic
- A firewall is deployed between networks: a private network and the internet for instance
- Firewalls filter traffic based on a set of rules: filters or Access Control Lists (ACL)
  - A set of instructions that distinguish authorized traffic from unauthorized and/or malicious traffic
- Firewalls are most effective against:
  - Unrequested traffic and attempts to connect from outside the private network
  - Known malicious data, messages, or packets based on content, application, protocol, port, or source address
  - They can hide the structure and addressing scheme of a network from the public

Firewalls

- Most firewalls offer:
  - Extensive logging, auditing, and monitoring capabilities
  - Alarms and basic intrusion detection system (IDS) functions
- Firewall logs many events about the network, system and itself:
  - Network traffic activity
  - A reboot of the firewall
  - Proxies or dependencies being unable to start or not starting
  - Proxies or other important services crashing or restarting
  - Changes to the firewall configuration file
  - Configuration or system error while the firewall is running
- Firewalls are typically unable to:
  - Block viruses or malicious code
  - Prevent unauthorized but accidental or intended disclosure of information by users
  - Prevent attacks by malicious users already behind the firewall
  - Protect data after it passes out of or into the private network
- Possible single point of failure: many of the security mechanisms are concentrated in one place

Firewalls

- Firewalls provide protection only against traffic that crosses the firewall from one subnet to another
  - They offer no protection against traffic within a subnet
- There are several basic types of firewalls:
  - Static packet-filtering firewalls
  - Application-level gateway firewalls
  - Circuit-level gateway firewalls
  - Stateful inspection firewalls
- Possibility to create hybrid or complex gateway firewalls

Firewalls: Static Packet-Filtering Firewalls

- A static packet-filtering firewall filters traffic by examining data from a message header
- The rules are concerned with source, destination, and port addresses
- Using static filtering, a firewall is unable to:
  - Provide user authentication
  - Tell whether a packet originated from inside or outside the private network
  - Easily fooled with spoofed packets
- Static packet-filtering firewalls are called screening routers and known as 1st generation firewalls
- They operate at layer 3 (the Network layer) of the OSI model

Firewalls: Application-Level Gateway Firewalls

- An application-level gateway firewall is also called a proxy firewall
- A proxy is a mechanism that copies packets from one network into another
  - It changes the source and destination addresses to protect the identity of the internal or private network
- It filters traffic based on the internet service used to transmit or receive the data
- Each type of application must have its own unique proxy server
- These firewalls negatively affects network performance:
  - Each packet must be examined and processed as it passes through the firewall
- Application-level gateways are known as 2nd generation firewalls
- They operate at the Application layer (layer 7) of the OSI model

Firewalls: Circuit-Level Gateway Firewalls

- Circuit-level gateway firewalls (aka circuit proxies) are used to establish communication sessions between trusted partners
- They operate at the Session layer (layer 5) of the OSI model
- SOCKS is a common implementation of a circuit-level gateway firewall
- Circuit-level gateway firewalls manage communications based on the circuit, not the content of traffic
- They permit or deny forwarding decisions based solely on the endpoint designations of the communication circuit
- They are considered as a 2nd generation firewalls because they represent a modification of the application-level gateway firewall concept

Firewalls: Stateful Inspection Firewalls

- Stateful inspection firewalls (aka dynamic packet filtering firewalls) evaluate the state or the context of network traffic, by examining:
  - Source and destination addresses,
  - Application usage,
  - Source of origin,
  - Relationship between current packets and the previous packets of the same session,
- Stateful inspection firewalls can:
  - Grant a broader range of access for authorized users and activities,
  - Actively watch for and block unauthorized users and activities.
- They are known as 3rd generation firewalls
- They operate at the Network and Transport layers (layers 3 and 4) of the OSI model

Firewalls: Deep Packet Inspection Firewalls

- Deep packet inspection (DPI) firewalls are filtering mechanisms that operate at the application layer
- DPI can also be known as complete packet inspection and information extraction (IX)
- DPI filtering can block domain names, malware, spam, or other identifiable elements in the payload of a communication
- DPI is often integrated with application layer firewalls and/or stateful inspection firewalls

Firewalls: Next-Gen Firewalls

- A next-gen firewall is a multifunction device (MFD) composed of several security features in addition to a firewall integrated components:
  - IDS,
  - Intrusion prevention system (IPS),
  - TLS/SSL proxy,
  - Web filtering,
  - QoS management,
  - Bandwidth throttling,
  - NATing,
  - VPN anchoring,
  - Antivirus.

Firewall Deployment Architectures

- There are three commonly recognized firewall deployment architectures:
  - single tier, two tier, and three tier (also known as multitier).
- Single tier deployment:
  - As shown in Figure 8.1, a single-tier deployment places the private network behind a firewall, which is then connected through a router to the internet
  - Single-tier deployments are useful against generic attacks and offer only a minimal protection

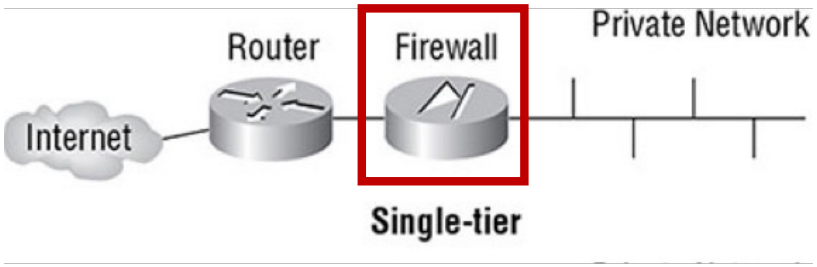


FIGURE 8.1 Single-tier firewall deployment architectures

Firewall Deployment Architectures

- A two-tier deployment: may be one of two different designs
  - One uses a firewall with 3 or more interfaces (figure 8.2), and the other uses 2 firewalls in a series (8.3)

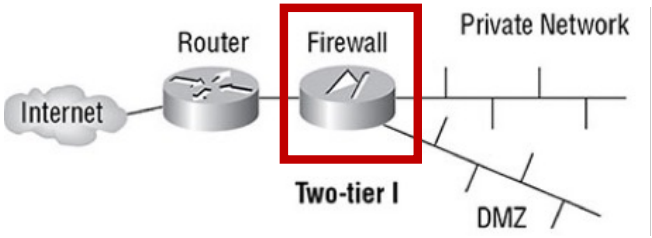


FIGURE 8.2 two-tier firewall deployment architectures type I

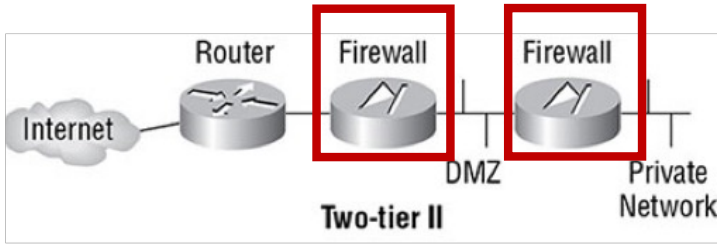


FIGURE 8.3 two-tier firewall deployment architectures type II

  - This allows for a DMZ or a publicly accessible extranet
  - In the first design, the DMZ is located off one of the interfaces of the primary firewall
  - In the second design, the DMZ is located between the two serial firewalls
  - The firewall routes traffic to the DMZ or the trusted network according to its filtering rules
  - This architecture introduces a moderate level of routing and filtering complexity

Firewall Deployment Architectures

- A three-tier deployment:
  - The deployment of multiple subnets between the private network and the internet separated by firewalls (Figures 8.4 and 8.5)
  - The outermost subnet is usually a DMZ
  - A middle subnet can serve as a transaction subnet where systems needed to support complex web applications in the DMZ reside
  - The third, or back-end, subnet can support the private network
  - This architecture is the most secure, but it is the most complex to design, implement, and manage

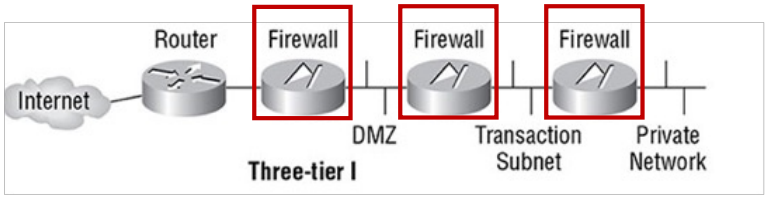


FIGURE 8.4 3-tier firewall deployment architectures type I

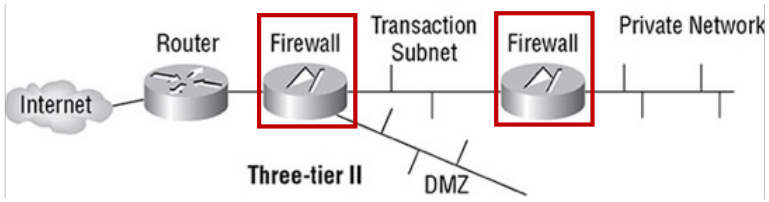


FIGURE 8.5 3-tier firewall deployment architectures type II

Endpoint Security

- Endpoints are the ends of a network communication link:
  - One end is often at a server where a resource resides
  - The other end is often a client making a request to use a network resource
- Endpoint security: each individual device must maintain local security whether or not its network or telecommunications channels also provide or offer security
- Sometimes this is expressed as "the end device is responsible for its own security"
- Using appliance firewalls, proxies, centralized virus scanners, and IDS/IPS/IDP solutions, to provide security for all of the network is no longer considered best business practices
- Lack of internal security is even more problematic
- Every system should have an appropriate combination of a local host firewall, anti-malware scanners, authentication, authorization, auditing, spam filters, and IDS/IPS services

Collaborations

Collaboration Tools

Secure Communication Protocols

- Internet Protocol security (IPsec) uses public key cryptography to provide
  - Primary for virtual private networks (VPN): IPsec can operate in either transport or tunnel mode
- Kerberos offers a single sign-on solution for users
  - Provides protection for logon credentials
- Secure Shell (SSH) is a good example of an end-to-end encryption technique:
  - Encrypts numerous plaintext utilities (rcp, rlogin, rexec,...),
- Signal Protocol:
  - A cryptographic protocol that provides end-to-end encryption for voice communications, videoconferencing, and text message services
- Secure Remote Procedure Call (S-RPC):
  - An authentication service and a means to prevent unauthorized execution of code on remote systems
- Secure Sockets Layer (SSL):
  - An encryption protocol to protect communications between a web server and a web browser
  - SSL can be used to secure web, email, File Transfer Protocol (FTP) or even Telnet traffic
  - SSL is superseded by Transport Layer Security (TLS)
- Transport Layer Security (TLS):
  - As SSL, but it uses stronger authentication and encryption protocols

Authentication Protocols

- Challenge Handshake Authentication Protocol (CHAP)
  - It used over Point-to-Point Protocol (PPP) links
  - CHAP encrypts usernames and passwords
  - It performs authentication using a challenge-response dialogue that cannot be replayed
  - CHAP also periodically reauthenticates the remote system
  - This activity is transparent to the user.
- Password Authentication Protocol (PAP)
  - This is a standardized authentication protocol for PPP
  - PAP transmits usernames and passwords in cleartext
  - It offers no form of encryption
  - It provides a means to transport the logon credentials from the client to the authentication server
- Extensible Authentication Protocol (EAP)
  - This is a framework for authentication instead of an actual protocol
  - EAP allows customized authentication security solutions: smart cards, tokens, and biometrics

Secure Voice Communications

- The vulnerability of voice communication is related to IT system security and the usage of digital devices and VoIP
- Confidentiality should be maintained by employing an encryption service or protocol
- Vulnerabilities of Normal private branch exchange (PBX) or POTS/public switched telephone network (PSTN)
- Inside security: Physical security is required to maintain control over voice communications within organization's physical locations
- Outside security: Security of voice communications outside your organization is the responsibility of the service provider

Voice over Internet Protocol (VoIP)

- VoIP is a technology that encapsulates audio into IP packets to support telephone calls over TCP/IP network connections
- Hackers can wage a wide range of potential attacks against a VoIP solution:
  - Caller ID can be falsified easily using any number of VoIP tools
  - A man-in-the-middle attacks by spoofing call managers or endpoint connection negotiations and/or responses.
- Secure Real-Time Transport Protocol or (SRTP) is a security improvement over the Real-Time Transport Protocol (RTP) used in many VoIP communications

Social Engineering

- Social engineering is a means by which an unknown, untrusted, or at least unauthorized person gains the trust of someone inside an organization
- Once convinced, the victim is often encouraged to make a change to their user account on the system, such as resetting their password
- Other attacks include instructing the victim to open specific email attachments, launch an application, or connect to a specific uniform resource locator (URL)
- People within an organization make it vulnerable to social engineering attacks

Multimedia Collaboration

- Multimedia collaboration is the use of various multimedia-supporting communication solutions to enhance distance collaboration
- Collaboration allows workers to work simultaneously as well as across different time frames
- Collaboration can incorporate:
  - Email, chat, VoIP, videoconferencing, use of a whiteboard, online document editing, real-time file exchange, versioning control, and other tools

Remote Meeting

- Remote meeting technology is used for any product, hardware, or software that allows for interaction between remote parties:
  - To communicate, exchange data, collaborate on materials/data/documents, perform work tasks
  - Aka: digital collaboration, virtual meetings, videoconferencing, software or application collaboration, shared whiteboard services, virtual training solutions, etc.
- Security implications must be evaluated:
  - Does the service use strong authentication techniques?
  - Does the communication occur across an open protocol or an encrypted tunnel?
  - Does the solution allow for true deletion of content?
  - Are activities of users audited and logged?
  - How about user data privacy?

Instant Messaging

- Instant messaging (IM) is a mechanism that allows for real-time text-based chat between two users located anywhere on the internet
- Some forms of IM are based on a peer-to-peer service while others use a centralized controlling server
- It's difficult to manage from a corporate perspective because it's generally insecure:
  - It's susceptible to packet sniffing,
  - It lacks true native security capabilities,
  - It provides no protection for privacy.

Manage Email Security

- The email infrastructure consists of:
  - Email servers using Simple Mail Transfer Protocol (SMTP):
    - To accept messages from clients,
    - To transport those messages to other servers,
    - To deposit them into a user's server-based inbox
  - Email clients that retrieve email from their server-based inboxes using Post Office Protocol version 3 (POP3) or Internet Message Access Protocol (IMAP)
  - Sendmail is the most common SMTP server for Unix systems
  - Exchange is the most common SMTP server for Microsoft systems

Manage Email Security

- Deploying an SMTP server requires to properly configure authentication for both inbound and outbound mail
- SMTP is designed to be a mail relay system that relays mail from sender to intended recipient
- SMTP server can serve as an open relay, which does not authenticate senders before accepting and relaying mail:
  - Open relays are prime targets for spammers
  - They allow spammers to send out floods of emails by piggybacking
- SMTP should be closed or authentication relays

Email Security Goals

- Adding security to email may satisfy one or more of the following objectives:
  - Provide for nonrepudiation
  - Restrict access to messages to their intended recipients (i.e., privacy and confidentiality)
  - Maintain the integrity of messages
  - Authenticate and verify the source of messages
  - Verify the delivery of messages
  - Classify sensitive content within or attached to messages
- Within the security policy, you must address several issues:
  - Acceptable use policies for email
  - Access control
  - Privacy
  - Email management
  - Email backup and retention policies

Understand Email Security Issues

- The lack of native encryption is one of the least important security issues related to email
- Email is a common delivery mechanism for viruses, worms, Trojan horses, documents with destructive macros, and other malicious code
- Hyperlinks within the content of email and attachments are a serious threat to every system
- Spoofing the source address of email is a simple process for even a novice attacker
- Email headers can be modified at their source or at any point during transit
- Mail servers are subject to Mail-bombing/email flooding, and spamming

Email Security Solutions

- Several protocols, services, and solutions to add security to email:
  - Without requiring a complete overhaul of the entire internet-based SMTP infrastructure
  - Examples: S/MIME, MOSS, PEM, and PGP
- Secure Multipurpose Internet Mail Extensions (S/MIME)
  - S/MIME is an email security standard that offers authentication and confidentiality to email through public key encryption and digital signatures
  - Authentication is provided through X.509 digital certificates
  - Privacy is provided using Public Key Cryptography Standard (PKCS) encryption
  - Two types of messages can be formed using S/MIME:
    - A signed message provides integrity, sender authentication, and nonrepudiation
    - An enveloped message provides integrity, sender authentication, and confidentiality

Email Security Solutions

- MIME Object Security Services (MOSS)
  - MOSS provides authentication, confidentiality, integrity, and nonrepudiation for email messages
  - MOSS employs Message Digest 2 (MD2) and MD5 algorithms, Rivest–Shamir–Adleman (RSA) public key, and Data Encryption Standard (DES)
- Privacy Enhanced Mail (PEM)
  - PEM is an email encryption mechanism that provides authentication, integrity, confidentiality, and nonrepudiation
  - PEM uses RSA, DES, X.509
- Domain Keys Identified Mail (DKIM)
  - DKIM is a means to assert that valid mail is sent by an organization through verification of domain name identity. (See http://www.dkim.org)
- Pretty Good Privacy (PGP)
  - PGP is a public-private key system that uses encryption algorithms (RSA, International Data Encryption Algorithm - IDEA, etc.) to encrypt files and email messages
  - PGP is not a standard but an independently developed product that has wide internet grassroots support

Virtualization

Virtual Private Network (VPN)

Virtual Local Area Network (VLAN)

Virtual software and virtual networking

Virtual Private Network (VPN)

- VPN is a communication tunnel that provides point-to-point transmission of authentication and data traffic over an intermediary untrusted network (Figure 9.)
- They do not provide or guarantee availability
- But encryption is not necessary for the connection to be considered as a VPN

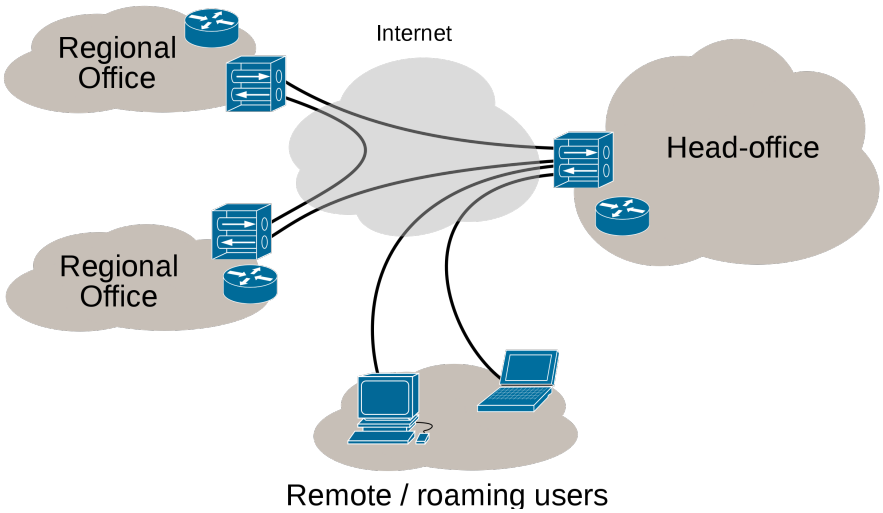


FIGURE 9 A VPN schema (source Wikipedia)

- The VPN can link two networks or two individual systems: Clients, servers, routers, firewalls, and switches.
- VPNs provide security for legacy applications that rely on risky or vulnerable communication protocols or methodologies
- VPNs also provide a sort of anonymity: hide your location

Tunneling

- Tunneling is the network communications process that protects the contents of protocol packets by encapsulating them in packets of another protocol
- A virtual path exists between the encapsulation and the de-encapsulation entities located at the ends of the communication
- Tunneling bypasses firewalls, gateways, proxies, or other traffic control devices
- The bypass is achieved by encapsulating the restricted content inside packets that are authorized for transmission

Tunneling

- Some issues:
  - Issue of latency:
    - Most protocols include their own error detection, error handling, acknowledgment, and session management features
    - Using more than one protocol at a time compounds the overhead required to communicate a single message
    - Tunneling creates either larger packets or additional packets
  - It can quickly saturate a network if sufficient bandwidth is not available
  - It is a point-to-point communication mechanism and is not designed to handle broadcast traffic
  - It is difficult, if not impossible, to monitor the content of the traffic in some circumstances

Layer 2 Forwarding Protocol and Layer 2 Tunneling Protocol

- Cisco developed its own VPN protocol called Layer 2 Forwarding (L2F):
  - A mutual authentication tunneling mechanism
  - L2F does not offer encryption
- L2F was not widely deployed and was soon replaced by L2TP
- Both can encapsulate any LAN protocol
- Layer 2 Tunneling Protocol (L2TP) was derived by combining elements from both PPTP and L2F
- L2TP creates a point-to-point tunnel between communication endpoints
- IPsec is commonly used as a security mechanism for L2TP
- L2TP also supports TACACS+ and RADIUS

IP Security Protocol (IPsec)

- The most used VPN protocol is IPsec
- IPsec is both a stand-alone VPN protocol and the security mechanism for L2TP
- IPsec has two primary functions:
  - Authentication Header (AH): for authentication, integrity, and nonrepudiation
  - Encapsulating Security Payload (ESP): for encryption, but it can perform a limited authentication
- It operates at the Network layer (layer 3) and can be used in transport mode or tunnel mode
- In transport mode, the IP packet data is encrypted but the header of the packet is not
- In tunnel mode, the entire IP packet is encrypted, and a new header is added to the packet

VPN Characteristics

TABLE 2 VPN characteristics.

VPN Protocol	Native Authentication Protection	Native Data Encryption	Protocols Supported	Dial-Up Links Supported	Number of Simultaneous Connections
PPTP	Yes	No	PPP	Yes	Single point-to-point
L2F	Yes	No	PPP/SLIP	Yes	Single point-to-point
L2TP	Yes	No (can use IPsec)	PPP	Yes	Single point-to-point
IPsec	Yes	Yes	IP only	No	Multiple

- VPN protocols which encapsulate PPP can support any subprotocol compatible with PPP (IPv4, IPv6, IPX, and AppleTalk)

Virtual Local Area Network (VLAN)

- VLAN is a hardware-imposed network segmentation created by switches
  - VLANs can also be assigned or created based on device MAC address
- VLAN management is most used to distinguish between user traffic and management traffic:
  - VLAN 1 very typically is the designated management traffic VLAN
- Communications between members of the same VLAN occur without hindrance
- Communications between VLANs require a routing function:
  - "deny by default; allow by exception" is a guideline for security in general
- VLANs are treated like subnets but aren't subnets
- VLANs are used to segment a network logically without altering its physical topology

OS Virtualization

- Virtualization technology is used to host one or more operating systems within a single host computer
- This mechanism allows virtually any OS to operate on any hardware
  - Examples: VMware/vSphere, Microsoft's Hyper-V, VirtualBox, XenServer, and Apple's Parallels
- Virtualized servers and services are indistinguishable from traditional servers and services from a user's perspective
- Virtualization is used for a wide variety of new architectures and system design solutions:
  - Cloud computing is ultimately a form of virtualization
  - Locally: host servers, client operating systems, limited user interfaces (i.e., virtual desktops), applications, etc.

OS Virtualization

- Virtualization has several benefits:
  - Being able to launch individual instances of servers or services as needed
  - Real-time scalability
  - Being able to run the exact OS version needed for the needed application
  - Recovery from damaged, crashed, or corrupted virtual systems is often quick:
  - Simply replace the virtual system's main hard drive file with a clean backup version and then relaunch it.
- In relation to security, virtualization offers several benefits:
  - It is easier and faster to make backups of entire virtual systems than the equivalent native hardware-installed system
  - When there is an error or problem, the virtual system can be replaced by a backup in minutes
  - Malicious code compromise or infection of virtual systems rarely affects the host OS
  - This allows for safe testing and experimentation → Sandboxing

OS Virtualization

- VM vulnerability: VM escaping
  - Occurs when software within a guest OS is able to breach the isolation protection of the hypervisor to violate the container of other guest OSs or to infiltrate the host OS
  - Example: Virtualized Environment Neglected Operations Manipulations (VENOM)
    - Breaches VM products that employed a compromised open-source virtual floppy disc driver to allow malicious code to jump between VMs and even access to the host
- VM escaping countermeasures:
  - Keep highly sensitive systems and data on separate physical machines
  - Keep all hypervisor software updated with vendor-released patches
  - Monitor attack, exposure, and abuse indexes for new threats to the environment

Virtual Networking

- A virtualized network or network virtualization is the combination of hardware and software networking components into a single integrated entity
- The resulting system allows for software control over all network functions: management, traffic shaping, address assignment, etc.
- A single management console or interface can be used to oversee every aspect of the network
- They allow organizations to implement or adapt other network solutions:
  - Software-Defined Networks, Virtual SANs (Storage Area Network), guest operating systems, and port isolation

Intrusion Detection Systems

Appendix

Intrusion Detection System – IDS

- Principles
- Goals
- Watch anomalies
- Requirements
- Why looking for detecting intrusions?
- Modeling behavior
- Vulnerabilities knowledge
- IDS origins of information
- Practical aspects
- Passive versus Active NIDS

Source: all this part of the lecture is extracted from Jacky Lemée cybersecurity courses.

Intrusion Detection System – IDS

- Watch traffic and events in a real-time or in differed-time to detect:
  - Working malfunctioning and abnormal behavior
  - External and internal attacks
- Host and Network IDS:
  - On host: HIDS components behavior analysis
  - On the network: NIDS: network traffic analysis
- Goal:
  - Alert to react if needed
  - Restrict the time delay for the attacker to act
- An IDS must come with regular analysis of its reports and logs

Intrusion Detection System – IDS

Anomaly Detection

- At the network level:
  - Unexplained significant level of traffic
  - Unusual ingoing or outgoing accesses with unusual sites/over busy network links
  - Complaining from users or from remote systems
- System alteration:
  - Files and directories altered, moved, modified
  - Missing recording in logs or accounting, deletion, inconsistency
- Unusual usages:
  - User profile modification, new user ID,
  - User abnormal activity (i.e., accounting who launched coding environment)
  - Resources over consumption: disk space, CPU time, etc.
  - Miscellaneous “errors”: login failure, security alarms,
  - Usage outside regular hours (at night for instance)

Intrusion Detection System – IDS

- Needs:
  - Stable and mastered environment
  - Logs: security, system, accounting
  - Adapted tools
  - Users and data processing
  - People contribution
  - Explain every event in the system: Find the origin of event, everything must be explained
- “By default” detection:
  - Company informed about the problem by its external customers!
  - Possible if:
    - An internal employee is involved
    - The company was a bounce relay without knowing that

Intrusion Detection System – IDS

- Why is it important to look for detecting intrusions?
  - It's impossible to provide a 100% guarantee of the security of a system:
    - Too costly, too complex
  - Same weaknesses appear on various systems:
    - Code vulnerabilities (example: ping of death)
    - Installation and configuration errors (permissions on files, …)
  - Difficult to keep equipment, OS or applications up to date in a real-time against news flaws
  - Firewalls are needed but don't process all the content of the traffic
  - Habits take precedence over security (Sendmail vs postfix)

IDS: two approaches

- Modeling behavior:
  - Learn the behavior of users, systems, applications to be able to notice deviating events that may indicate an unusual (attempt of privilege abuse, spoofing, etc.) event
  - Neuron networks
- Vulnerability knowledge:
  - Take benefit skilled security knowledge to look for attempts to use flaws
    - Signature analysis
    - Expert systems

IDS: origins of information

- On the host HIDS
  - Logs and audit trails watching (audit C2, syslog,…)
  - Resources requests
  - Logs may be altered by attackers
- On the network NIDS
  - Packet analysis:
    - Is the packet compliant with the security policy?
    - Is the packet part of a known attack?
  - Losses of packets possible
- From applications:
  - Activity log analysis (web servers, databases, etc.)

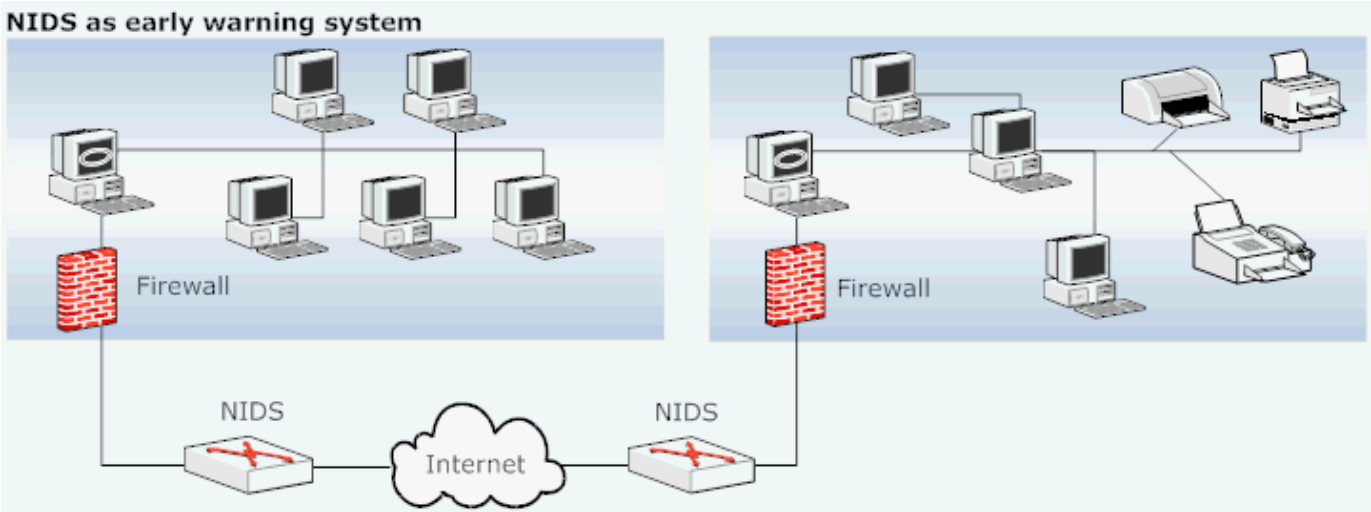
IDS: Practical aspect

- Most IDS on the market look for attack characteristics events (signature analysis) by listening and analyzing the network
- They lead to problems of:
  - Attack Knowledge exhaustivity (up to date signature bases)
  - Efficiency of packets capture
- Installation requires a learning phase to train the IDS in front of the environment
  - False positive: event wrongly considered as abnormal,
  - False negative: attack event undetected by IDS

IDS: Passive vs Active NIDS

- Passive NIDS:
  - Watches the traffic on the network segment to which the NIDS is attached
  - Apart alerts generation, takes no actions when a flow is considered as suspicious
    - It is recommended to use a passive NIDS when the rate of false positive may be high: flows not under control, network traffic heavy
- Active NIDS:
  - Watches the traffic on the network segment AND may interrupt sessions considered as suspect
  - The mechanism used to end a TCP session generally leans on an RST packet sent to pretend to be one of the extremities of the TCP communication,
    - It implies an address spoofing
    - It is recommended to use an active NIDS when false positive are rare: controlled flows, network traffic low or medium

IDS: Passive vs Active NIDS



Source: https://www.cse.wustl.edu/~jain/cse571-07/ftp/ids/

- Watch interface:
  - The interface of the NIDS must be activated in “promiscuous” mode to give to the NIDS the TCP/IP stack it needs to work on
- IP routing:
  - “IP forwarding” between the various network interfaces of the NIDS must be deactivated (NO IP FORWARDING)
- Administration flow:
  - Connection between the NIDS network administration interface and the administration server machine must go through the filtering components

Further reading

- https://www.ssi.gouv.fr/en/publications/:
  - Dozens of free publications in all domains of cybersecurity from ANSSI (in English)
  - Compliance with the French/EU regulation in the matter
- https://www.enisa.europa.eu/publications
  - Numerous free publications in all domains of cybersecurity from ENISA (in English)
  - Compliance with the EU regulation in the matter
- Mike Chapple, James Michael Stewart, Darril Gibson. **(ISC)2 CISSP® Certified Information Systems Security Professional**. Official Study Guide. Eighth Edition. O'Reilly Media, Inc. 2020.
- Elad Elrom. **The Blockchain Developer. A Practical Guide for Designing, Implementing, Publishing, Testing, and Securing Distributed Blockchain-based Projects**. ISBN 978-1-4842-4846-1e-ISBN 978-1-4842-4847-8. https://doi.org/10.1007/978-1-4842-4847-8 © Elad Elrom 2019
- https://www.cse.wustl.edu/~jain/cse571-07/ftp/ids/#sec2