# INFO 6010 Lesson 8
# Communication & Network Security – Part 2
# Domain 4

**Revision 2**

Information Security Management & Network Security and Architecture

FANSHAWE

# Discussion Topics - Part Two

- Network components and services
- Communications security management
- Remote access technologies
- Threats and attacks
- Software-defined networks
- Content distribution networks
- Multilayer protocols
- Convergent network technologies

# Network Components

- Several types of devices are used in LANs, MANs, and WANs to provide intercommunication between computers and networks
  - Repeaters
  - Bridges
  - Routers
  - Switches

# Repeaters

- A repeater provides the simplest type of connectivity
- Repeaters work at the physical layer and are add-on devices for extending a network
- Repeater amplifies signals
- Repeaters can also work as line conditioners by cleaning signals
- Hub is a multiport repeater

# Repeaters

- Hubs are often referred to as *Concentrators*
- Hub does not understand or work with IP or MAC addresses
- When one host sends a signal to another system the signal is broadcast to all ports on the hub
- Hubs are susceptible to collisions in large networks, and performance issues

# Bridges

- Bridge is a LAN device used to connect LAN segments
- Bridge works at the data link layer and therefore works with MAC addresses
- When a frame arrives at a bridge it determines whether or not the MAC address is on the local network segment
- If MAC address is not on the local network segment bridge forwards the frame to the necessary network segment

# Bridges

- Bridge is used to divide busy networks into smaller segments to ensure better use of bandwidth and traffic control
- Susceptible to broadcast storms
- Segments a large network into smaller
- Filtering traffic based on MAC addresses
- Joins different types of network links while retaining the same broadcast domain

# Bridges

- **Forwarding Tables**
- A bridge must know how which port the frame must be sent and where the destination host is located
- This is accomplished by **“transparent bridging”**
- A bridge starts to learn about the network’s environment as soon as it is powered on
- Examines frames and makes entries in its forwarding table
- When bridge receives a frame from a new source computer it associates new source address and the port on which it arrived
- If bridge receives a request to a destination that is not in its forwarding table it sends out a query frame on each network segment except for the source segment

# Bridges

- **Bridges use the Spanning Tree Algorithm (STA)**
- STA ensures that frames do not circle networks forever
- Provides redundant paths in case a bridge goes down
- Assigns unique identifiers to each bridge
- Assigns priority values to bridges
- Calculates path costs

# Routers

- Routers are OSI Layer 3 (Network Layer) devices
- Used to connect similar or different networks
- A router is a device that has two or more interfaces and a routing table
- Router can filter traffic based on access control lists (ACLs)
- Router can fragment packets when necessary
- Routers are smarter devices which are capable of calculating the shortest and most economical path between the sending and receiving hosts
- Router discovers information about routes through routing protocols (RIP, BGP, OSPF)

# Router Decisions

1. A frame is received, router views the routing data
2. Router retrieves the destination IP network address from the datagram
3. Router looks at its routing table to see which port matches the requested destination IP network address
4. If the router does not have information in its table about the destination address it sends out an ICMP error message to the sending computer indicating that the message could not reach its destination

# Router Decisions

5. If the router does have a route in its routing table for this destination it decrements the TTL value and sees whether the MTU is different for the destination network. If the destination network requires a smaller MTU, the router fragments the datagram.
6. The router changes header information in the frame so the frame can go to the next correct router or
7. The router sends the frame to its output queue for the necessary interface.

# Switches (1)

- Switches combine the functionality of a repeater and the functionality of a bridge
- Switch is a multiport bridging device
- Each port provides dedicated bandwidth to the device attached to it
- A port is bridged to another port so the two devices have an end-to-end private link

# Switches (2)

- Switch employs full-duplex communication (one wire pair is used for sending and another pair is used for receiving)
- Basic switches work at the data link layer and forward traffic based on MAC addresses
- More advanced higher-level switches offer routing functionality, packet inspection, traffic prioritization and QoS functionality

# Switches (3)

- **Layer 3 and 4 Switches**
- Distinction between layer 2, 3, and 4 switches is the header information the device looks at to make forwarding or routing decisions
  - data link, network, or transport OSI layers
  - Layer 2 switches forward a frame based on its MAC Address
- Layer 3 and 4 switches can use tags which are assigned to each destination network or subnet
- Tagging process increases the speed of routing of packets from one location to another
- Provides a level of QoS
  - Class of Service IEEE 802.1q
- Addresses service requirements for the different packet types (Video)

# Switches - VLANs

- **VLANs**
- Virtual LANs enable administrators to separate and group computers logically based on resource requirements, security, or business needs instead of the standard physical location of the systems
- A VLAN exists on top of the physical network
- Multiple VLANS can be configured on a physical switch
- Each VLAN is a broadcast domain ( IP subnet)
- No packet flow between VLANs unless packet sent to router first
- VLAN's utilize packet tagging
  - IEEE 802.1Q protocol
  - Inserts a field into Ethernet header that contains VLAN id of frame
  - Also contains a 3 bit field for CoS (Class of Service)

# Gateways

- *Gateway* is a general term for software running on a device that connects two different environments and acts as a translator for them or restricts their interactions.
- Usually a gateway is needed when one environment speaks a different language, meaning it uses a certain protocol that the other environment does not understand.
- The gateway can translate Internetwork Packet Exchange (IPX) protocol packets to IP packets, accept mail from one type of mail server, and format it so another type of mail server can accept and understand it, or it can connect and translate different data link technologies such as FDDI (Fiber Distributed Data Interface) to Ethernet.

# PBXs

- Telephone companies use switching technologies to transmit phone calls to their destinations.
- A *Private Branch Exchange (PBX)* is a private telephone switch that is located on a company’s property. This switch performs some of the same switching tasks that take place at the telephone company’s central office. The PBX has a dedicated connection to its local telephone company’s central office, where more intelligent switching takes place.

# Firewalls

- Firewalls are used to restrict access to one network from another network
- A firewall device supports and enforces the company's network security policy
- Firewall is described as a "choke point" in the network because all communication should flow through it and this is where traffic is inspected and restricted
- A firewall may be a router, server, or specialized hardware device
- Firewall filters out the packets that do not meet the requirements of the security policy
- Packets can be filtered based on their source and destination addresses and ports by service, packet type, protocol type, header information, sequence bits, and more

# Firewalls

- **Packet-Filtering Firewalls**
- Packet filtering is a security method of controlling what data can flow into and out of a network
- Packet filtering takes place by using ACLs
- Rules applied to each packet it receives
- Filtering is based on network layer information
- Filtering decisions based on header information
- Packet-filtering firewalls also do not keep track of the state
- Packet filtering is the method used by the first-generation firewall

# Firewalls

- **Do not** prevent attacks that employ application-specific vulnerabilities or functions
- The logging functionality present in packet-filtering firewalls is limited
- Most packet-filtering firewalls do not support advanced user authentication schemes
- Many packet-filtering firewalls cannot detect a network packet in which the OSI layer 3 addressing information has been altered (spoofed)

# Stateful Firewalls

- Stateful inspection filtering remembers and keeps track of what packets were sent where until each particular connection is closed
- Stateful-inspection firewall is nosier than a regular filtering device because it keeps track of what computers say to each other
- Requires that the firewall maintain a state table
- Stateful inspection firewalls work at the network and transport layers
- Stateful-inspection firewalls can be victims of many types of Denial-of-Service (DoS) attacks
- When state table is stuffed full of bogus information device may either freeze or reboot

# Proxy Firewalls

- Proxy intercepts and inspects messages before delivering them to the intended recipients
- Proxy accepts messages either entering or leaving a network
- Proxy inspects them for malicious information and passes the data on to the destination computer
- Proxy firewalls are second-generation firewalls
- A proxy firewall stands between a trusted and untrusted network and makes the connection each way on behalf of the source
- Proxy firewall makes a copy of each accepted packet before transmitting it
- Proxy repackages the packet to hide the packet’s true origin
- Proxy firewall is the only machine that talks to the outside world

# Application Level Proxy Firewalls

- *Application-level proxies* inspect the packet up through the application layer. Where a circuit level proxy only has insight up to the session layer, an application-level proxy understands the packet as a whole and can make access decisions based on the content of the packets.
- An application-level proxy firewall has one proxy per protocol. A computer can have many types of protocols. Thus, one application-level proxy per protocol is required. So one portion of the firewall product is dedicated to understanding how a specific protocol works and how to properly filter it for suspicious data.

# Dynamic Packet-Filtering Firewalls

- An internal system communicates with an entity outside its trusted network, it chooses a source port so the receiving system knows how to respond properly.
  - Ports up to 1023 are called *well-known ports* and are reserved for specific server-side services. The sending system must choose a dynamic port higher than 1023 when it sets up a connection with another entity.
- The *dynamic packet-filtering firewall* creates an ACL that allows the external entity to communicate with the internal system via this high-numbered port. If this were not an available option for the dynamic packet-filtering firewall, it will have to allow “punch holes” in the firewall for all ports above 1023, because the client side chooses these ports dynamically and the firewall would never know exactly on which port to allow or disallow traffic.

# Kernel Proxy Firewalls

- A *kernel proxy firewall* is considered a fifth-generation firewall. It creates dynamic, customized network stacks when a packet needs to be evaluated.
- When a packet arrives at a kernel proxy firewall, a new virtual network stack is created, which is made up of only the protocol proxies necessary to examine this specific packet properly.
- If it is an FTP packet, then the FTP proxy is loaded in the stack. The packet is scrutinized at every layer of the stack. This means the data link header will be evaluated along with the network header, transport header, session layer information, and the application layer data. If anything is deemed unsafe at any of these layers, the packet is discarded.

# Next Generation Firewalls

- A **next-generation firewall** (**NGFW**) combines a traditional firewall with other network device filtering functionalities, such as an application firewall using in-line deep packet inspection (DPI), an intrusion prevention system (IPS). Other techniques might also be employed, such as TLS/SSL encrypted traffic inspection, website filtering, QoS/bandwidth management, antivirus inspection and third-party identity management integration (i.e. LDAP, RADIUS, Active Directory).
- The typical cost of ownership alone tends to make these infeasible for small or even medium-sized networks.

# Firewalls

- **Bastion Host**
- Bastion host is just another name for a locked-down (or hardened) system
- A bastion host is a highly exposed device
- Typically front line in a network's security and its existence is known on the Internet
- Any system that resides within the DMZ should be installed on a bastion host

# Firewalls

- **Dual-Homed Firewall**
- Dual-homed refers to a device that has two interfaces
  - one facing the external network
  - one facing the internal network
- Common multihomed firewall architecture allows multiple DMZs

# Firewalls

- **Screened Host**
- A screened host is a firewall that communicates directly with a perimeter router and the internal network
- Traffic received from the Internet is first filtered via packet filtering on the outer router
- Traffic that makes it past this phase is sent to the screened-host firewall
- Screened-host firewall applies more rules and drops denied packets

# Firewalls

- **Screened Subnet**
- A screened-subnet architecture adds another layer of security to the screened-host architecture
- External firewall screens the data entering the DMZ network
- Traffic is passed to an internal firewall which also filters the traffic
- The use of these two physical firewalls creates a DMZ

# Firewalls

- **Firewalls Fundamentals**
- The default action of any firewall should be to implicitly deny any packets not explicitly allowed
  - If no rule states that the packet can be accepted packet should be denied
- Any packets entering the network that have a source address of an internal host should be denied
- No traffic should be allowed to leave a network that does not have an internal source address (egress filtering)
- Firewalls should reassemble fragmented packets before being sent on to their destination

# Firewalls

- **The following list addresses some of the disadvantages of firewalls:**
- Most of the time a distributed approach needs to be used to control all network access points, which cannot happen through the use of just one firewall
- Firewalls can present a potential bottleneck to the flow of traffic
- Firewalls can restrict desirable services that users may want to access
  - (See: Corporate Security Policy)

# Firewalls

- **The following list addresses more of the disadvantages of firewalls:**
- Most firewalls do not provide protection from viruses being downloaded or passed through e-mail, and hooks to virus-detection techniques are needed
- Border firewalls provide little protection against the inside attacker
- Firewalls do not protect against rogue modems in listening mode
- Firewalls do not protect against rogue wireless access points

# Proxy Servers

- A **proxy server** is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.
- A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity.

# Unified Threat Management

- **Unified threat management** (**UTM**) is an approach to information **security** where a single hardware or software installation provides multiple **security** functions. This contrasts with the traditional method of having point solutions for each **security** function.
- Some issues with implementing UTM products are:
  - **Single point of failure for traffic** Some type of redundancy should be put into place.
  - **Single point of compromise** If the UTM is successfully hacked, there may not be other layers deployed for protection.
  - **Performance issues** Latency and bandwidth issues can arise since this is a “choke point” device that requires a lot of processing.

# Content Distribution Networks

- A **content distribution network** (**CDN**) is a geographically distributed network of proxy servers and their data centers. The goal is to provide high availability and high performance by distributing the service spatially relative to end-users.
- CDNs serve a large portion of the Internet content today, including web objects (text, graphics and scripts), downloadable objects (media files, software, documents), applications (e-commerce, portals), live streaming media, on-demand streaming media, and social media sites.

# Software Defined Networking

- **Software-defined networking** (**SDN**) technology is an approach to network management that enables dynamic, programmatically efficient network configuration in order to improve network performance and monitoring making it more like cloud computing than traditional network management.
- SDN is meant to address the fact that the static architecture of traditional networks is decentralized and complex while current networks require more flexibility and easy troubleshooting. SDN attempts to centralize network intelligence in one network component by disassociating the forwarding process of network packets (data plane) from the routing process (control plane). The control plane consists of one or more controllers which are considered as the brain of SDN network where the whole intelligence is incorporated. However, the intelligence centralization has its own drawbacks when it comes to security, scalability and elasticity and this is the main issue of SDN.

# End Points

- An *endpoint* is any computing device that communicates through a network and whose principal function is not to mediate communications for other devices on that network.
    - If the device is connected to a network but is not part of the routing, relaying, or managing of traffic on that network, then it is an endpoint.

# Honeypots

- A honeypot system is a computer that usually sits in the screened subnet or DMZ and attempts to lure attackers to it instead of to actual production computers
- Network administrators want to keep the attackers away from their other systems and set up honeypots as decoys
- Administrators would keep detailed logs, enable auditing, and per- form different degrees of forensics in the hopes of turning over the attackers to the authorities for prosecution

# Network Access Control

- **Network Access Control** (**NAC**) attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication  and network security enforcement by using policies, including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do.

# Virtualized Networks

- Routers and switches can be virtualized by deploying software products that carry out routing and switching functionality.
- They behave like the physical counterparts.
- VM’s can save money, power, heat and physical space.
  - The greatest strength of the VM is the hypervisor but also its greatest weakness. As it could be a single point of weakness and therefore subject to attack.
  - Keep up to date with security patches.
  - Beware of third-party add-ons that extend the functionality of the hypervisor or virtual infrastructure.
  - Ensure these are well tested and acquired from reputable vendors.

Lastly, ensure that whoever provisions and maintains the virtualized infrastructure is competent and diligent.

# Intranets and Extranets

- When a company uses web-based technologies that are only available inside its networks, it is using an *intranet*, a “private” network.
  - The company has web servers and client machines using web browsers, and it uses the TCP/IP protocol suite. The web pages are written in HTML or XML (eXtensible Markup Language) and are accessed via HTTP.
- An *extranet* extends outside the bounds of the company’s network to enable two or more companies to share common information and resources. Business partners commonly set up extranets to accommodate business-to-business communication.

# Metropolitan Area Network (MAN)

- Usually a backbone that connects LANs to each other and LANs to WANs
- LAN’s to the Internet and telecommunications and cable networks
- Majority of today’s MANs are Synchronous Optical Networks (SONETs) or FDDI rings provided by the telecommunications service providers
- Businesses can connect to the rings via T1, fractional T1, and T3 lines
- SONET ring and the devices usually necessary to make this type of communication possible
- SONET is actually a standard for telecommunications transmissions over fiber-optic cables
- SONET is self-healing - if a break in the line occurs it can use a backup redundant ring to ensure transmission continues

# Wide Area Networks

- Wide area network (WAN) technologies are used when communication needs to travel over a larger geographical area
- **CSU/DSU**
- A Channel Service Unit/Data Service Unit (CSU/DSU) is required when digital equipment will be used to connect a LAN to a WAN. This connection can take place with T1 and T3 lines
- CSU/DSU is necessary because the signals and frames can vary between the LAN equipment and the WAN equipment
- DSU device converts digital signals from routers, bridges, and multiplexers into signals that can be transmitted over the telephone company's digital lines

# WAN

- **CSU/DSU**
- DSU device ensures that the voltage levels are correct and that information is not lost during the conversion
- CSU connects the network directly to the telephone company’s line
- CSU/DSU is not always a separate device and can be part of a networking device
- CSU/DSU basically works as a translator and, at times, as a line conditioner

# Multiplexing

- In telecommunications and computer networks, multiplexing is a method by which multiple analog or digital signals are combined into one signal over a shared medium. The aim is to share a scarce resource. E.g. in telecommunications, several telephone calls may be carried using one pair of wires.

# Switching

- **Dedicated links** have one single path to traverse
- Two points of reference are needed when a packet leaves one network and heads toward the other
- Much more complicated when thousands of networks are connected to each other
- Two types of switching can be used:
  - **Circuit switching**
  - **Packet switching**

# Switching

- **Circuit switching**
  - Creates a virtual connection that acts like a dedicated link between two systems
  - **Example:** ISDN and telephone calls are examples of circuit switching
- **Packet switching**
  - Does not set up a dedicated virtual link
  - Packets from one connection can pass through a number of different individual devices
  - **Example**: The Internet and Frame Relay are examples of packet switching

# Frame Relay

- Frame relay is a WAN protocol that operates at the data link layer
- A packet switching technology to let multiple companies and networks share the same WAN media
- Frame relay cost is based on the amount of bandwidth used
- Because several companies and networks use the same media cost is reduced per company compared to dedicated links
- Companies pay for a portion of available bandwidth that is always available to the Committed Information Rate, CIR
- **Equipment used in frame relay connections:**
  - Data Terminal Equipment (DTE) – Customer owned device
  - Data Circuit-Terminating Equipment (DCE) – Service Provider owned device

# Frame Relay

- **Virtual Circuits**
  - Frame relay (and X.25) forward frames across virtual circuits These circuits can be either permanent or switched
- **Permanent Virtual Circuit** (PVC)
  - Works like a private line for a customer with an agreed-upon bandwidth availability
  - PVC provides a guaranteed level of bandwidth, it does not have the flex- ibility of an SVC
- **Switched Virtual Circuits** (SVCs)
  - Require steps similar to a dial-up and connection procedure
  - SVCs are used for teleconferencing, establishing temporary connections to remote sites, data replication, and voice calls

# X.25

- X.25 is an older WAN protocol similar to Frame Relay
- X.25 is a packet switching technology
  - Many users use the same service simultaneously
- Provides an any-to-any connection
- Subscribers are charged based on the amount of bandwidth
- Packet size128 bytes and encapsulated in High-level Data Link Control (HDLC) frames
- HDLC frames are addressed and forwarded across the carrier switches

# Asynchronous Transfer Mode - ATM

- Asynchronous Transfer Mode (ATM) is a switching technology
- It uses a cell-switching
- ATM is a high-speed networking technology used for LAN, MAN, WAN, and service provider connections
- Similar to Frame relay it is a connection-oriented switching technology
- Creates and uses a fixed channel
- Data is segmented into fixed-size cells of 53 bytes instead of variable-size packets
- ATM sets up virtual circuits, which act like dedicated paths between the source and destination
- Virtual circuits can guarantee bandwidth and QoS
- ATM is a good carrier for voice and video transmission

# ATM

- **Quality of Service**
- Quality of Service (QoS) is a capability that allows a protocol to distinguish between different classes of messages and assign priority levels
- QoS allows a service provider to guarantee a level of service to its customers

# ATM

- Four different types of ATM QoS services are available
- **Constant Bit Rate (CBR)**
  - A connection-oriented channel that provides a consistent data throughput for time-sensitive applications, such as voice and video applications. Customers specify the necessary bandwidth requirement at connection setup
- **Variable Bit Rate (VBR)**
  - A connection-oriented channel best used for delay-insensitive applications because the data throughput flow is uneven. Customers specify their required peak and sustained rate of data throughput
- **Unspecified Bit Rate (UBR)**
  - A connectionless channel that does not promise a specific data throughput rate. Customers cannot, and do not need to, control their traffic rate
- **Available Bit Rate (ABR)**
  - A connection-oriented channel that allows the bit rate to be adjusted. Customers are given the bandwidth that remains after a guaranteed service rate has been met

# ATM

- **QoS has three basic levels:**
- **Best- effort service**
  - No guarantee of throughput, delay, or delivery
  - Traffic that has priority classifications goes before traffic that has been assigned this classification
  - Most of the traffic that travels on the Internet has this classification
- **Differentiated service**
  - Compared to best-effort service, traffic that is assigned this classification has more bandwidth, shorter delays, and fewer dropped frames
- **Guaranteed service**
  - Ensures specific data throughput at a guaranteed speed
  - Time-sensitive traffic (voice and video) is assigned this classification

FANSHAWE

# SDLC and HDLC

- Synchronous Data Link Control is a computer communications protocol. It is the layer 2 protocol for IBM's Systems Network Architecture. SDLC supports multipoint links as well as error correction. It also runs under the assumption that an SNA header is present after the SDLC header.
- High-Level Data Link Control is a bit-oriented code-transparent synchronous data link layer protocol developed by the International Organization for Standardization. HDLC provides both connection-oriented and connectionless service.

# Point - to - Point Protocol (PPP)

- Point - to - Point Protocol (PPP) is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers. It is a byte - oriented protocol that is widely used in broadband communications having heavy loads and high speeds. Since it is a data link layer protocol, data is transmitted in frames.
- The main services provided by Point - to - Point Protocol are −
  - Defining the frame format of the data to be transmitted.
  - Defining the procedure of establishing link between two points and exchange of data.
  - Stating the method of encapsulation of network layer data in the frame.
  - Stating authentication rules of the communicating devices.
  - Providing address for network communication.
  - Providing connections over multiple links.
  - Supporting a variety of network layer protocols by providing a range of services.

# Multiservice Access Technologies

- Multiservice access technologies combine several types of communication categories (data, voice, and video) over one transmission line
- Provides higher performance, reduced operational costs, and greater flexibility, integration, and control for administrators
- Basic phone system is based on a circuit-switched, voice-centric network, referred to as the public-switched telephone network (PSTN)

# Multiservice Access Technologies

- When a phone call is made, the connection has to be set up, signaling has to be controlled, and the session has to be torn down
- When Voice over IP (VoIP) is used, it employs the Session Initiation Protocol (SIP), which sets up and breaks down the call sessions
- PSTN is being replaced by data-centric, packet-oriented networks that can support voice, data, and video

# H.323 Gateways

- H.323 is an ITU Telecommunication Standardization Sector (ITU-T) recommendation that describes protocols for the provision of audio-visual (A/V) communication sessions on all packet networks. H.323 provides standards for equipment, computers and services for multimedia communication across packet based networks and specifies transmission protocols for real-time video, audio and data details.
- It is widely used in IP based videoconferencing, Voice over Internet Protocol (VoIP) and Internet telephony. Users can communicate through the Internet and make use of a variety of products that are H.323 standard compatible.

# Session Initiation Protocol - SIP

- **Session Initiation Protocol**
- Signaling protocol widely used for VoIP communications sessions
- It is used in applications such as video conferencing, multimedia, instant messaging, and online gaming
- SIP relies on a three-way-handshake process to initiate a session
- SIP itself is not used to stream the conversation because it’s just a signaling protocol
- Actual voice stream is carried on media protocols such as the Real-time Transport Protocol (RTP)

# SIP

- SIP consists of two major components:
- **User Agent Client (UAC)**
  - Application that creates the SIP requests for initiating a communication session
  - Generally messaging tools and soft-phone applications that are used to place VoIP calls
- **User Agent Server (UAS)**
  - UAS is the SIP server
  - Responsible for handling all routing and signaling involved in VoIP calls

# SIP

- SIP architecture constitutes of three different types of servers
  - **Proxy server**
  - **Registrar server**
  - **Redirect server**
- *Proxy server* is used to relay packets within a network between the UACs and the UAS
- *Registrar server* keeps a centralized record of the updated locations of all the users on the network
- *Redirect server* allows SIP devices to retain their SIP identities despite changes in their geographic location

# IP Telephony

- **IP Telephony Issues**
- VoIP’s integration with TCP/IP protocol has same security challenges
- Allows malicious users to bring their TCP/IP
- VoIP systems use operating systems, communicate through Internet protocols
- SIP-based signaling suffers from the lack of encrypted call channels and authentication of control signals

# IP Telephony

- **IP Telephony Issues**
- Attackers can tap into the SIP server and client communication to sniff out login IDs, passwords/PINs, and phone numbers
- Toll fraud is considered to be the most significant threat that VoIP networks face
- Attackers can also masquerade identities by redirecting SIP control packets from a caller to a forged destination to mislead the caller into communicating with an unintended end system
- VoIP devices are vulnerable to DoS attacks

# VoIP Security

- Hackers can intercept incoming and outgoing calls, carry out DoS attacks, spoof phone calls, and eavesdrop on sensitive conversations
- Many of the countermeasures to these types of attacks are the same ones used with traditional data oriented networks:
- Keep patches updated
  - The call manager server
  - The voicemail server
  - The gateway server
- Identify unidentified or rogue telephony devices
  - Implement authentication so only authorized telephony devices are working on the network

# VoIP Security

- Install and maintain:
  - Stateful firewalls
  - VPN for sensitive voice data
  - Intrusion detection
- Filter unnecessary ports on routers, switches, PCs, and IP telephones
- Employ real-time monitoring that looks for attacks, tunneling, and abusive call patterns through IDS/IPS
- Employ content monitoring
- Use encryption when data (voice, fax, video) cross an untrusted network
  - Use a two-factor authentication requirement
  - Limit the number of calls via media gateways
  - Close the media sessions after completion

# Remote Access

- Remote access covers several technologies that enable remote and home users to connect to networks that will grant them access to network resources that help them perform their tasks
- Most common types of remote connectivity methods used are VPNs, dial-up connections, ISDN, cable modems, and DSL connections
- When you are looking at the security angle of remote access, the three most important rules to enforce are the following:
- All users on the remote access equipment must be fully authenticated to proceed with its use
- No covert or inappropriate access to the communication circuits is allowed
- After authentication, users shall have access to those authorized services to which they are entitled, and no more

# Remote Access

- **Dial-Up and RAS**
- Remote access is usually gained by connecting to a remote access server (RAS), which acts as a gateway and can be an endpoint to a PPP session
- Users dial into a RAS which performs authentication by comparing the provided credentials with the database of credentials it maintains
- Access authentication technology used in remote connection situations is RADIUS

# Remote Access

- **Wardialing**
- Used by many attackers to identify remote access modems
- Specially written program tools can be used to dial a large bank of phone numbers
- Tools log valid data connections and attempt to identify the system
- Wardialing enables an attacker to find all the modems that provide remote access into a network

# ISDN

- **Integrated Services Digital Network (ISDN)**
- Communications protocol provided by telephone companies and ISPs
- Enable data, voice, and other types of traffic in a digital manner
- ISDN uses the same wires and transmission media used by analog dial-up technologies but it works in a digital fashion
- ISDN provides two basic home and business services:
  - **Basic Rate Interface (BRI)**
  - **Primary Rate Interface (PRI)**

# ISDN

- **BRI**
- Has two B channels that enable data to be transferred
- Has one D channel that provides for call setup, connection management, error control, caller ID
- Bandwidth available with BRI is 144 Kbps
- BRI service is common for residential use
- **PRI**
- Has 23 B channels and one D channel and is more common in business

# DSL

- **Digital Subscriber Line (DSL)**
- High-speed connection technology used to connect a home or business to the service provider’s central office
- Can provide 6 to 30 times higher bandwidth speeds than ISDN and analog technologies
- Uses existing phone lines and provides a 24-hour connection to the Internet\
- Distance limited have to be within a 2.5-mile radius of the DSL service provider’s equipment

# DSL

- DSL is a broadband technology that can provide up to a 52-Mbps transmission
- As residence and the central office distance increases the transmission rates for DSL decrease
- DSL provides faster transmission rates because it uses all of the available frequencies available on a voice-grade UTP line
- **DSL offers several types of services:**
  - Symmetric services - traffic flows at the same speed upstream and downstream
  - Asymmetric services - downstream speed is higher than upstream speed

# VPNs

- **Virtual Private Network (VPN)**
- Secure and private connection through a public network or an otherwise unsecure environment
- Private connection because the encryption and tunneling protocols are used to ensure the confidentiality and integrity of the data in transit
- Protocols that can be used for VPNs are Point-to-Point Tunneling Protocol (PPTP), IPSec, and L2TP
- Sending and receiving ends must have the necessary hardware and software to set up an encrypted tunnel
- Remote users can use VPNs to connect to their company network to access their e-mail, network resources, and corporate assets

# VPNs

- VPNs use tunneling protocols
- A tunnel is a virtual path across a network that delivers packets that are encapsulated and possibly encrypted
- Tunneling protocols encapsulate one protocol in another protocol to be properly routed over specific networks
  - IPX, NetBEUI and AppleTalk
- Three main tunneling protocols are used in VPN connections:
  - **PPTP**
  - **L2TP**
  - **IPSec**

# VPNs

- **Virtual Private Network (VPN)**
- Secure and private connection through a public network or an otherwise unsecure environment
- Private connection because the encryption and tunneling protocols are used to ensure the confidentiality and integrity of the data in transit
- Protocols that can be used for VPNs are Point-to-Point Tunneling Protocol (PPTP), IPSec, and L2TP
- Sending and receiving ends must have the necessary hardware and software to set up an encrypted tunnel
- Remote users can use VPNs to connect to their company network to access their e-mail, network resources, and corporate assets

# Point-T0-Point Tunneling Protocol

- **PPTP** is a Microsoft protocol that allows remote users to set up a PPP connection to a local ISP and then create a secure VPN to their destination
- Packet payload is encrypted with Microsoft Point-to-Point Encryption (MPPE) using MS-CHAP or EAP-TLS
- Keys used in encrypting this data are generated during the authentication process between the user and the authentication server
- PPTP can work only over IP networks

# Layer 2 Tunneling Protocol

- **L2TP** provides the functionality of PPTP but it can work over networks other than just IP
- Provides a higher level of security when combined with IPSec
- L2TP does not provide any encryption or authentication services
- Encapsulation process is similar to PPTP
- If destination system receives an L2TP frame it processes the headers and IPSec trailer
- Then verifies the integrity and authentication of the frame

# PPTP vs L2TP

- PPTP can run only within IP networks. L2TP can run within and tunnel through networks that use other protocols like frame relay, X.25 and ATM
- PPTP is an encryption protocol and L2TP is not. L2TP lacks the security to be called a true VPN solution. L2TP is often used in conjunction with IPSec to provide the necessary encryption
- L2TP supports TACACS+ and RADIUS while PPTP does not

# Authentication Protocols

- **Password Authentication Protocol (PAP)**
  - Used by remote users to authenticate over PPP lines
  - Provides identification and authentication
  - Requires a user to enter a password before being authenticated
  - Password and the username credentials are sent over the network to authentication server compares supplied credentials to its database
  - PAP is one of the least secure authentication methods because credentials are sent in clear text

# Authentication Protocols

- **Challenge Handshake Authentication Protocol (CHAP)**
  - Addresses some of the vulnerabilities found in PAP
  - Uses a challenge/response mechanism to authenticate the user instead of sending a password
  - Server sends the user a challenge (random value)
  - Challenge is encrypted with predefined password and the encrypted challenge value is returned to the server

# Network Encryption

- ***Link encryption*** encrypts all the data along a specific communication path, as in a satellite link, T3 line, or telephone circuit. User information, header, trailers, addresses, and routing data that are part of the packets are also encrypted.
- Link encryption provides protection against packet sniffers and eavesdroppers.
- Link encryption, (*online encryption)*, is usually provided by service providers and is incorporated into network protocols.
- All of the information is encrypted, and the packets must be decrypted at each hop so the router, or other intermediate device, knows where to send the packet next. The router must decrypt the header portion of the packet, read the routing and address information within the header, and then re-encrypt it and send it on its way.

# Network Encryption

- In ***end-to-end encryption***, the headers, addresses, routing information, and trailer information are not encrypted, enabling attackers to learn more about a captured packet and where it is headed.
- With end-to-end encryption, the packets do not need to be decrypted and then encrypted again at each hop because the headers and trailers are not encrypted. The devices in between the origin and destination just read the necessary routing information and pass the packets on their way.
- End-to-end encryption is usually initiated by the user of the originating computer. It provides more flexibility for the user to be able to determine whether or not certain messages will get encrypted. It is called "end-to-end encryption" because the message stays encrypted from one end of its journey to the other. Link encryption has to decrypt the packets at every device between the two ends.

# Network Encryption

- Advantages of link encryption include:
  - All data is encrypted, including headers, addresses, and routing information.
  - Users do not need to do anything to initiate it. It works at a lower layer in the OSI model.

- Disadvantages of link encryption include:
  - Key distribution and management are more complex because each hop device must receive a key, and when the keys change, each must be updated.
  - Packets are decrypted at each hop; thus, more points of vulnerability exist.

# Encryption at different Layers

- Encryption can happen at different layers of an operating system and network stack:
  - End-to-end encryption happens within the applications.
  - TLS encryption takes place at the session layer.
  - PPTP encryption takes place at the data link layer.
  - Link encryption takes place at the data link and physical layers.

# E-mail Encryption Standards

- **Email encryption** is encryption of email messages to protect the content from being read by entities other than the intended recipients.
- Email is prone to the disclosure of information. Most emails are currently transmitted in the clear (not encrypted).

# E-Mail Stds

- Multipurpose Internet Mail Extension (MIME)
  - Is a technical specification indicating how multimedia data and e-mail attachments are to be transferred
  - If a message or document contains a binary attachment, MIME dictates how that portion of the message should be handled
  - MIME is a specification that dictates how certain file types should be transmitted and handled
- Secure MIME (S/MIME)
  - Standard for encrypting and digitally signing electronic mail and for providing secure data transmissions
  - Extends the MIME standard by allowing for the encryption of e-mail and attachments

# E-Mail Stds

- Pretty Good Privacy (PGP)
  - Designed by Phil Zimmerman as a freeware for e-mail security
  - PGP is a complete cryptosystem that uses cryptographic protection to protect e-mail and files
  - Uses RSA public key encryption for key management
  - Uses IDEA symmetric cipher for bulk encryption
  - PGP does not use a hierarchy of CA’s

# E-Mail Stds

- PGP relies on a “web of trust” in its key management
  - Each user generates and distributes his or her public key
  - MIT provides a key ring
  - PGP is a public domain software that uses public key cryptography.
  - Product free for individuals to use, it has become somewhat of an encryption de facto standard on the Internet.

# Internet Security - HTTP

- HTTP
  - TCP/IP is the protocol suite of the Internet
  - HTTP is the protocol of the Web
  - HTTP sits on top of TCP/IP
- Browser uses HTTP to send a request to the web server hosting the web site
- Web server sends the requested file to user via HTTP
- HTTP is a stateless protocol this means the client and web server establish and close a connection for each send/receive operation

# Internet Security - HTTPS

- HTTP Secure (HTTPS)
  - HTTP run with SSL
  - Secure Sockets Layer (SSL)
- Uses public key encryption and provides data encryption
- SSL provides
  - Server authentication
  - Message integrity
  - Client authentication

# Internet Security - HTTPS

- Server and client negotiate security parameters
- Server authenticates to the client by sending it a digital certificate
- Client checks the certificate and the process continues
- Client generates a session key and encrypts it with the server’s public key
- Both use this symmetric key to encrypt the data

- Note: SSL is generally regarded as obsolete and insecure!

# Cookies

- Cookies are text files that a browser maintains on a user’s hard drive
- Created by web servers and written to PC
- Cookies have different uses
  - Information about users last connection to the web site
  - Shopping cart
- HTTP is a stateless protocol, meaning a web server has no memory of any prior connections
  - Store session id
  - Time stamp for expired connections

# Cookies

- Server should encrypt sensitive data in cookies
- Can prevent server from storing cookies on hard drive

# Secure Shell - SSH

- SSH is a program and a protocol that can be used to log into another computer over a network
- Provide a secure and encrypted tunnel between two computers
- When two computers complete handshaking process and exchange session key that will be used during to encrypt and encrypt data
- SSH should be used instead of Telnet, FTP, rlogin, rexec, or rsh

# Network Attacks

- Network security attacks are unauthorized actions against private, corporate or governmental IT assets in order to destroy them, modify them or steal sensitive data. As more enterprises invite employees to access data from mobile devices, networks become vulnerable to data theft or total destruction of the data or network.
- There are two main types of network attacks:
- **Passive:** this is when sensitive information is screened and monitored, potentially compromising the security of enterprises and their customers.
- **Active:** this is when information is altered by a hacker or destroyed entirely.

# Network Attacks

- A **denial-of-service attack** (**DoS attack**) is a cyber-**attack** in which the perpetrator seeks to make a machine or **network** resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.
- **Malformed Packet**
- A ping of death (“POD”) attack involves the attacker sending multiple malformed or malicious pings to a computer. The maximum packet length of an IP packet (including header) is 65,535 bytes.

# Network Attacks

- A distributed denial of service (DDoS) attack is a malicious attempt to make an online service unavailable to users, usually by temporarily interrupting or suspending the services of its hosting server.
- A DDoS attack is launched from numerous compromised devices, often distributed globally in what is referred to as a botnet, the intention is to flood the target with malicious traffic.

# Network Attacks

- **Ransomware** is a subset of malware in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access is returned to the victim.
- The motive for ransomware attacks is nearly always monetary, and unlike other types of attacks, the victim is usually notified that an exploit has occurred and is given instructions for how to recover from the attack.
- Payment is often demanded in a virtual currency, such as Bitcoin, so that the cybercriminal's identity is not known.

# Network Attacks - Sniffing

- A sniffer is an application that can capture network packets.
- Sniffers are also known as network protocol analizers.
- While protocol analyzers are really network troubleshooting tools, they are also used by hackers for hacking network.
- If the network packets are not encrypted, the data within the network packet can be read using a sniffer.
- Sniffing refers to the process used by attackers to capture network traffic using a sniffer.
- Once the packet is captured using a sniffer, the contents of packets can be analyzed.
- Sniffers are used by hackers to capture sensitive network information, such as passwords, account information.

# Network Attacks

***DNS hijacking*** is an attack that forces the victim to use a malicious DNS server instead of the legitimate one. The techniques for doing this fairly simple and fall into one of three categories:

- **Host based** Conceptually, this is the simplest hijacking attack in that the adversary just changes the IP settings of the victim's computer to point to the rogue DNS server. Requires physical or logical access to the target and typically calls for administrator privileges on it.
- **Network based,** the adversary is in your network, but not in the client or the DNS server. A technique such as ARP table cache poisoning could be used to redirect DNS traffic to the attackers server.
- **Server based** If the legitimate DNS server is not configured properly, an attacker can tell this server that his own rouge server is the authoritative one for whatever domains he wants to hijack. Thereafter, whenever the legitimate server receives a request for the hijacked domains, it will forward it to the rogue server automatically.

# Network Attacks

- A **Drive-by Download** refers to the unintentional download of malicious code onto a computer or mobile device that exposes users to different types of threats. Cybercriminals make use of drive-by downloads to steal and collect personal information, inject banking Trojans, or introduce exploit kits or other malware to endpoints, among many others.
- Users need not click on anything to initiate the download. Simply accessing or browsing a website can activate the download.
- The malicious code is designed to download malicious files onto the victim's device without the user being aware that anything untoward has happened.

# Homework

- Read the relevant chapter in the set book ‘All In One CISSP Exam Guide’ – by Shon Harris.

- Communication & Network Security
- Go through the Quick Tips at the end of the chapter

- Then identify and do the practice m/c questions relating to this subject, these will either be at the end of the chapter if you are using the current edition or spread between different chapters in earlier editions.

# Questions

- ?