Infrastructure Security

Chapter 10

Background

- Security failures
  - A failure allows unauthorized users to access resources and data.
    - This compromises integrity or confidentiality.
  - Failure prevents authorized users from accessing resources and data.
    - This is often overlooked.
- The primary goal of network infrastructure security is to allow all authorized use and deny all unauthorized use of resources.

Network Infrastructure

- More than just client computers and servers.
  - Devices
  - Media
  - Security Concerns for Transmission Media
  - Removable Media
  - Security Topologies
  - Tunneling

Devices

- Devices
  - Connect the client and servers together, and regulate the traffic between them.
  - Helps in expanding the network beyond simple client computers and servers to include other devices
- Types of Devices:
  - Workstations
  - Servers
  - Hubs
  - Switches
  - Routers
  - Wireless access points
  - VPN devices.

Workstation Security

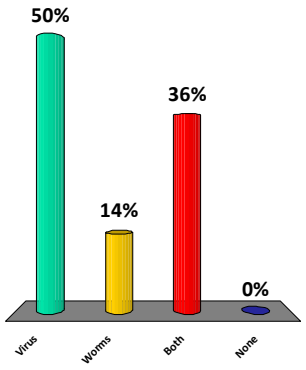
- Workstations
  - The client computers in a client/server model.
  - Used everyday for tasks like e-mail, application programs, games
  - If on a network, an important part of security
- Virus –
  - A piece of software that is introduced into a network and then executed on a machine.
  - Can easily spread across machines in a network.
  - For viruses, workstations are the primary mode of entry into a network.
- The two most common ways
  - Transfer of an infected file from one machine to another.
    - Floppies, CDs, or FTP. When the transferred file is executed, the virus is propagated.
  - E-mail
- Worms
  - Software that do not require a file transfer
  - Can move from machine to machine without file transfer operations

Workstations

- Increase Workstation security:
  - Remove unnecessary protocols such as Telnet, NetBIOS, and IPX.
  - Remove modems unless needed and authorized.
  - Remove all unnecessary share privileges.
  - Rename the administrator account and add a strong password.
  - Remove unnecessary user accounts.
  - Install an antivirus program and keep it up-to-date.
  - Remove or disconnect the floppy drive if not needed.
  - Ensure the presence of a firewall between the machine and the Internet.
  - Keep the OS patched and up-to-date.

_____ are software that attaches itself to a file and then executes on a machine

1. Virus
2. Worms
3. Both
4. None



Server Security

- Servers
  - Computers that host shared applications and data.
    - Web servers
    - Database servers
    - Email Servers
    - File servers
    - Print servers
  - The key management issue behind running a secure server setup is to identify the specific needs of a server for its proper operation and enable only items necessary for those functions
  - Server operating systems are more robust than a workstation system.
  - Serve multiple users.

Server Security

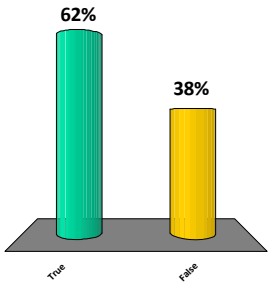
- Key Management issues:
  - Secure server setup requires identification of specific needs of the server.
  - All other services and users should be off the system to improve the system security.
    - Remove unnecessary protocols.
      - Examples: Telnet, NetBIOS, IPX, and FTP.
    - Remove unnecessary shares.
    - Rename the administrator account.
      - Secure using a strong password.
    - Keep the OS patched and up-to-date.
    - Control physical access.
  - **After a server has been built, record MD5 checksums on all crucial files.- Why??**

Server Antivirus Software

- Antivirus protection on servers depends upon the use of the server.
  - Email server - extensive antivirus protection
  - File server – need protection
  - For servers, this type of software is most useful when users are allowed to place files on the machine.
    - Domain controller and remote access server - may not require antivirus solution
      - do not allow user to place file on them

Workstation operating systems are more robust than a server system.

1. True
2. False



Network Interface Card (NIC)

- It is the physical connection between a computer and the network.
- Each NIC has unique code built in, called a Media Access Control (MAC) address, that is assigned by the manufacturer.
  - 48 bits long, with 24 bits representing the manufacturer and 24 bits being a serial number, guaranteeing uniqueness.
  - MAC addresses are used in the addressing and delivery of network packets to the correct machine and in a variety of security situations.
    - These addresses can be changed, or "spoofed," rather easily.
    - In fact, it is common for personal routers to clone a MAC address to allow users to use multiple devices over a network connection that expects a single MAC.

Hubs and Bridges

- **Hubs**
  - Allow multiple systems to be connected in a star configuration (Hub in the center).
    - All the connections share a single collision domain.
    - Hubs are signal conditioners that connect multiple devices to a common signal.
    - Increase in traffic causes collision
    - Insecure—all PCs connected to a hub see all of the traffic that passes through it.
  - Replaced by low-cost switches
- **Bridges**
  - Also connect devices using the same protocol at the physical layer of the OSI.
  - Reduce collisions by separating pieces of a network into separate collision domains.
    - Each cuts the collision problem into half.
  - Have been replaced by switches

A collision occurs when two or more network devices are trying to transmit packets at the exact same time.

Switches

- **Switches**
  - Creates separate collision domains for each port.
  - Can perform security functions
    - Help inspect packet headers and enforce access control lists (ACL- series of rules governing if a packet is allowed or not).
  - A sniffer can only see traffic for the connected port.
  - Subject to ARP poisoning and MAC flooding.

- **ARP poisoning:**
  - A device spoofs the MAC address of another device, attempting to change the ARP tables through spoofed traffic and the ARP table-update mechanism

- **MAC flooding**
  - A switch is bombarded with packets from different MAC addresses, flooding the switch table and forcing the device to respond by opening all ports and acting as a hub.
  - This enables devices on other segments to sniff the traffic

Switch Administration and security

- Securing a Switch
  - Disable a port so that it cannot be used without authorization
  - Port security- A feature which allows the administrators to control which systems can send data to each of the port
  - Disable all access protocols other than a serial line, or use Secure Shell (SSH).
  - Using secure access methods limits the exposure to hackers and malicious users.
  - Maintaining secure network switches is more important than securing individual boxes.

Routers

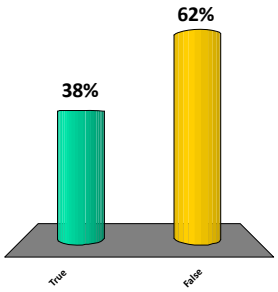
- Routers form the backbone of the Internet.
  - Traffic management devices used to connect different network segments together
    - Move traffic from network to network.
  - Forms the backbone of the Internet
  - Inspect packets from every communication as they move optimized traffic.
  - Examine each packet for destination addresses.
    - Determine where to send a packet using algorithms and tables.
    - May examine the source address and determine whether to allow a packet to pass.
  - Can also be attacked due to vulnerabilities in both SNMP and Telnet

Router Security

- A security concern of routers - access to its internal functions.
  - A router may be accessed using SNMP and be programmed remotely.
  - Physical control and security of router is absolutely necessary.
    - If a router is physically accessed by a hacker, it is compromised.
  - Ensure that administrative passwords are never passed.
    - Secure mechanisms are used to access the router.
    - Default passwords are reset to strong passwords.

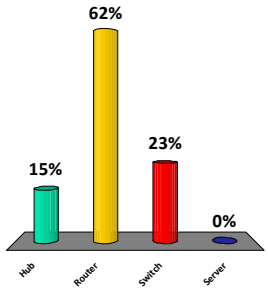
Switches create one big collision domain for all connected devices

1. True
2. False



You are building a small network in the office. You will need to connect two different network segments that have different network addresses. What device will you use connect them?

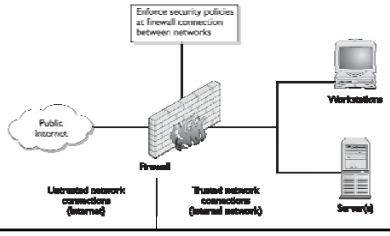
1. Hub
2. Router
3. Switch
4. Server



Firewalls

- A firewall is a network device - hardware, software, or a combination.
- It enforces a security policy across its connections.
  - Security policy - A series of rules that define what traffic is permissible and what traffic is to be blocked or denied.
  - A key to security policies - the principle of least access.
  - Only allow the necessary access for a function, and block or deny all unneeded functionality.
    - For example, a web server connected to the Internet may be configured only to allow traffic on port 80 for HTTP.

A corporate connection to the Internet should pass through a firewall to block all unauthorized network traffic



How Do Firewalls Work?

- Firewalls enforce established security policies through various mechanisms, including:
  - Network Address Translation (NAT)
  - Basic packet filtering
  - Stateful packet filtering
  - Access Control Lists (ACLs)
  - Application layer proxies

- Network Address Translation (NAT)
  - Allows masking of significant amounts of information from outside the network.
    - Hide internal IP address
  - Allows an outside entity to communicate with an entity inside the firewall without knowing its address.

Firewalls contd.

- Basic packet filtering
  - Checks each packet against rules pre-defined on the firewall
  - Fairly simple, fast, and efficient
  - Doesn't detect and catch all undesired packets

- Stateful packet filtering
  - The firewall maintains the context of a conversation
  - More likely to detect and catch undesired packets
  - Due to overhead, network efficiency is reduced

Firewalls contd.

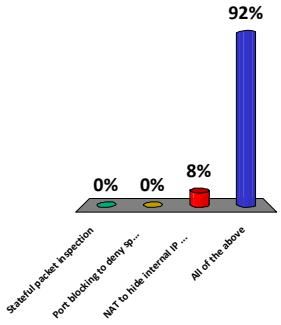
- Access Control Lists
  - Cornerstone of security in firewalls.
  - ACLs provide physical access control for electronic access.
  - Implies the list of IP addresses that have access to which ports and systems through the firewall.
- Application Layer Firewalls
  - Employ application layer proxies through which packets are not allowed to traverse the firewall,
  - But data instead flows up to an application that in turn decides what to do with it.

Best Practices for Firewalls

- All traffic from trusted network is allowed out
- Firewall device never directly accessed from public network
- Simple Mail Transport Protocol (SMTP) data allowed to pass through firewall
  - SMTP is a protocol used for email exchange
- Internet Control Message Protocol (ICMP) data denied
- When Web services offered outside firewall, HTTP traffic should be denied from reaching internal networks

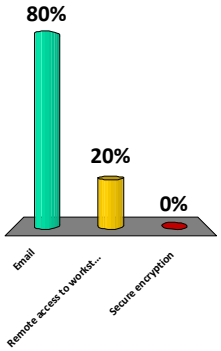
Firewalls can use which of the following in their operations

1. Stateful packet inspection
2. Port blocking to deny specific services
3. NAT to hide internal IP addresses
4. All of the above



SMTP is a protocol used for which of the following functions

1. Email
2. Remote access to workstations
3. Secure encryption



Wireless

- Wireless - additional security concerns.
  - No physical connection to a wireless device allows anyone within range to access the data.
  - Placing wireless devices behind a firewall stops only physically connected traffic from getting to the device.
- The point of entry from a wireless device to a wired network is a wireless access point.
  - Supports multiple concurrent devices accessing the network.
- Basic network security for connections can be performed by forcing authentication and verifying authorization.
- Wired Equivalent Privacy (WEP).
  - WEP is designed to prevent wireless sniffing of network traffic over the wireless portion of the network.

Modems

- Modem is short for modulator/demodulator.
  - Modems convert analog signals to digital and vice versa.
- DSL modem
  - Provides a direct connection between a subscriber's computer and an Internet connection at the local telephone company's switching station.
- Cable modems provide shared arrangements.
  - Other people can sniff traffic between the user and the ISP.
- DSL modems provide a direct connection.
  - Traffic cannot be sniffed between the user and the ISP.

Cable and DSL Modems

- Both cable and DSL services provide a continuous connection, which brings up the question of IP address life for a client.
  - Most services have a Dynamic Host Configuration Protocol (DHCP) to manage their address space.
- The most common security device used in cable/DSL connections is a firewall that should be installed between the cable/DSL modem and the client computers.
  - Two common methods are to install software on each client device or to use a cable/DSL router with a built-in firewall.
  - These can be combined with software for an additional level of protection.

Telecom/PBX

- Private branch exchanges (PBXs)
  - PBXs are computer-based switching equipment designed to connect telephones into the local phone system.
  - Can be compromised from the outside and used by phone hackers (phreakers) to make phone calls at the organization's expense.
  - Cause a problem when interconnected with data systems by corporate connection or rogue modems belonging to users.
    - Either case creates a path for connection to the outside data networks and the Internet.

VPN

- Provides a secure channel between users even though their signal is traveling on public networks
- Employs one of two types of encryption
  - Data encryption can be sniffed en route, but the contents cannot be read
  - Packet encryption uses tunneling and protects the data and the identities of the communicating parties
- The most common implementation of VPN is via IPsec, a protocol for IP security.
  - IPsec can be implemented in hardware, software, or a combination of both and is used to encrypt all IP traffic.

Intrusion Detection Systems

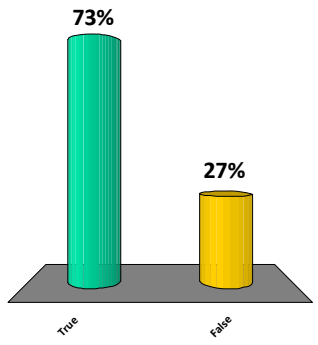
- Intrusion Detection Systems (IDS) :
  - Systems designed to detect, log, and respond to unauthorized network or host use, both in real time and after the fact
- The two categories :
  - Network-based systems
  - Host-based systems
- The two primary methods of detection :
  - Signature-based
  - Anomaly-based

Network Monitoring/Diagnostic

- When things start to go wrong, as in the case of a virus or worm attack, the network management become a busy and stressful place as operators attempt to return the system to full efficiency while not interrupting existing traffic
- Simple Network Management Protocol (SNMP) provides management, monitoring, and fault resolution on a network.
  - Used for remote access to network infrastructure
  - SNMP is the main standard embraced by vendors to permit interoperability.
- SNMP has holes in its implementation that should be taken into account when using it as part of a network monitoring solution.

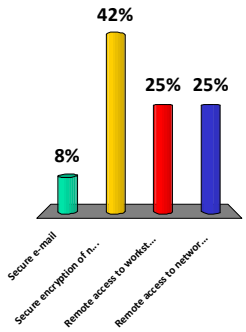
A virtual private network (VPN) is a construct used to provide Secure communication channel between users across public networks such as the Internet

1. True
2. False



SNMP is a protocol used for the following function

1. Secure e-mail
2. Secure encryption of network packet
3. Remote access to workstations
4. Remote access to network infrastructure



Mobile Devices

- Mobile Devices
  - Add several challenges for network administrators.
  - Can act as transmission vectors for viruses
  - Can be used to remove sensitive material offsite

Common Concerns in Device Security

- Default passwords are known to hackers, and frequently left unchanged

Physical Layer- Media

- The base of communications between devices is the physical layer of the OSI model
- It is the domain of the actual connection between devices, whether by wire, fiber, or RF waves.
- Methods of Connection
  - There are four common methods of connecting equipment at the physical layer:
    - Coaxial cable
    - Twisted-pair cable
    - Fiber optics
    - Wireless

Coax

- Coaxial cable
  - Familiar as a method of connecting televisions to VCRs or to satellite or cable services.
- Has high-bandwidth and shielding capabilities
- Less prone to outside interference than other cabling methods
- Vulnerable to “vampire taps”
  - Drilling a hole through the outer part of a coax cable and connect to the central connector
  - Easy method to get access to the signal & data being transmitted

UTP/STP

- Single pairs of twisted wires reduce electrical crosstalk.
- Two types:
  - **Shielded twisted-pair (STP)** has a foil shield around pairs to reduce electromagnetic interference.
  - **Unshielded twisted-pair (UTP)** relies on the twist to eliminate interference.
- Security Concerns:
  - Ease of connection
  - Easy to splice and rogue connections for sniffing

Fiber

- The most expensive cable option
- Used as the backbone medium of the Internet and large networks
- Is the hardest cable to splice
  - Unauthorized connections are all but impossible to make.
- The high cost make it less attractive for the final mile in public networks where users are connected to the public switching systems.
  - Cable companies use coax and DSL providers use twisted-pair to handle the "last-mile" scenario.

Unguided Media

- Unguided media covers all transmission media not guided by wire, fiber, or other constraints.
  - It includes radio frequency (RF), infrared (IR), and microwave methods.
- Unguided media have one attribute in common: they are unguided and as such can travel to many machines simultaneously.
  - Security principles are even more critical, as they must assume that unauthorized users have access to the signal.

Security Concerns for Transmission Media

- Things to avoid:
  - Access to a server by an unauthorized individual
  - Access to switches and routers by an unauthorized individual
  - Access to network connections by an unauthorized individual

Physical Security Concerns

- Limiting access to physical media to avoid the use of sniffers
- Properly securing wireless networks
- Use of either authenticated firewalls or VPNs

Removable Media

- The potential loss of control of the data on the moving media.
- The risk of introducing unwanted items, such as a virus or a worm, when the media are attached back to a network.

- Hard drives
  - Portable hard drives are physically small but have large capacities.
  - They can be used with encryption technology to protect the data if the drive is lost or stolen (particularly important for laptops).

- Electronic Media
  - High capacity, but small in size.
  - Becoming ubiquitous: laptops and PCs have built-in card readers
  - Can be used to move information between machin

Network Attached Storage

- Speed of today's Ethernet networks, has made possible to manage data storage across the network.
- This has led to a type of storage known as **Network Attached Storage (NAS).**
  - The combination of inexpensive hard drives, fast networks, and simple application-based servers has made NAS devices in the terabyte range affordable for even home users.
- High-capacity devices are accessed via the network

- Susceptible to various attacks:
  - Sniffing of credentials
  - Brute-force attacks to access the data