Mississippi State UNIVERSITY

J. A. "Drew" Hamilton, Jr., Ph.D.

Director, Center for Cyber Innovation

Professor, Computer Science & Engineering

CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu

Technologies & Tools

Reference:

Drew Hamilton Lecture Notes

DeMarcus Thomas

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

Domain Outline

- Network Components
- Security Tools and Technologies
- Troubleshooting Common Security Issues
- Mobile Devices
- Implementing Secure Protocols

Network Components Technologies & Tools

Reference:

Drew Hamilton Lecture Notes

DeMarcus Thomas

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

Network Components

- Systems today are composed of a number of highly interconnected parts
- These components work together to provide very complex operations in a synergistic manner
- Third party components will be introduced into this integrated system and will have security and risk implications
- This section is designed to provide an understanding of how components fit into an overall system design

Firewalls

- Allows the support of security policies that are defined by an organization
- The principle of least privilege should be followed to make sure only what needs to be done can be achieved
- Allows the filtering of network traffic at the port, packet, or application level

Firewalls cont.

- Goal is to protect the target of the attack before packets can reach it

- To develop a comprehensive security policy, specially for the firewalls, an organization must have an understanding of the resources that are available and how they are normally used in the network
  - A well configured firewall can detect and mitigate abnormal network activity such as DoS/DDoS attacks

How do firewalls work?

- **Firewalls enforces security policies through a number of different methods:**
  - **Network Address Translation**
  - **Basic packet filtering**
  - **Stateful packet filtering**
  - **Access control lists (ACLs)**
  - **Application layer proxies**

NATs

- Key idea is that outside devices can't communicate with internal devices directly
  - This was a IPv4 feature, but will probably be carried on to IPv6
  - Provides the ability to mask content from those outside of the network
  - Attacks from the outside will be directed towards the NAT device and not the target system

- Provides benefit of not needing as many public IP addresses

Basic packet filtering

- Filters traffic based on information within the packet
  - Source or destination IP address
  - Port
  - Protocols
- For certain devices, such as a database server, specific protocols can be allowed and other will be blocked
  - E.g. FTP or Telnet
- This method is simple and fast, but won't catch all undesired packets

Firewall Rules

- These rules provide specific instructions that support the overall policies that are being enforced
- Rules will vary from place to place depending on the constraints of the policy that is desired
- Structure of rules can range from simple to very complex
  - Can act on IP addresses or ports for either granting or denying access

ACLs

- Lists of users and the actions they are allowed to perform
- Examples
  - Used on file systems to manage who has access to resources
  - Used by router to determine what addresses are permitted
- Users can be identified by user ID, network address, or a token

Explicit denies with ACLs

- **Simple security principle when configuring firewalls**
  - **If access is not granted with a permit statement, then the final answer should be "deny all"**
- **This covers any other scenarios that could allow entry into the network**
- **ACL entries are normally examined from a top down approach**
  - **Any traffic that is not permitted will be dropped**

Application based vs. Network Based

- **Application layer firewall**
  - Checks traffic at a very deep level
    - Can check for specific characteristics of an application's traffic and block specific actions
  - Can create rules that are very granular, but are costly to efficiency
- **Network based firewall**
  - Use IP addresses and ports for filtering
  - Processes information quickly but is limited in what can be inspected
- **Trade off between performance and speed**

Application Firewalls cont.

- **Highly sensitive firewalls may use application layer proxies**
  - **Packets will not traverse the firewall, but will be forwarded to applications for a decision on what to do next**

- **Example**
  - **Simple Mail Transfer Protocol proxies**
    - **Accepts inbound mail from the Internet and then makes a decision on if it should be sent to the internal corporate mail server**

- **Extra capability is countered by performance degradation**

Stateful vs Stateless

- **Basic packet filtering is an example of stateless interaction**
  - **Actions based on IP addresses and ports**
- **Stateful filtering takes into account the "conversation" that is being had**
  - **Does this packet belong to an existing conversation or is it something new**
- **Stateful filtering provides more features and protection, but at the cost of speed**

Stateful vs stateless cont.

- **Stateful filtering helps to address attacks such as the following:**
  - **Packets that come from outside the network, in an attempt to pretend that it is a response to a message from inside the network**
  - **Should external access attempts from high port addresses be allowed or blocked**

Implicit deny for firewall rules

- All devices must have an implicit deny
  - All rules on a firewall are viewed in a top-down manner
  - Any permit or deny statements end the processing of a packet
  - This makes the order of the rules important

- All firewalls should end with a deny-all statement
  - If you make it to the last rule, where no other rules allowed the packet, deny it.

Secure Network Administration Principles

- Used to ensure network security is being supported
- Includes the actions of keeping hardware, software, configurations, and maintenance up to date
- Make sure that the policies for planning, design, and operations are security focused

Rule-Based Management

- This strategy takes the ideas of policies that should be followed and puts them into a concrete plan
- Applied in a number of settings including: firewalls, proxies, switches, router, anti-malware, IDS/IPS, etc.
- Each packet shown to a control device applies and interprets its predefined rules

VPN Concentrator

- VPN endpoint that is responsible for managing multiple communication connections at the same time
  - Each conversation is independent of one another
- VPNs offers a means of cryptographically securing a communication channel and a concentrator is the endpoint for the activity
- Device is designed to allow multiple connections across a single device and simplifies network architecture and security

Remote Access vs Site-to-Site

- **Both of these VPN designs provide the same support and protection of your data over the Internet**
  - **Main difference is in why they are being setup**

- **Remote access**
  - **Allows for remote users to connect to the network as needed**
- **Site-to-site**
  - **Allows for a dedicated connection between two systems**

IPSec

- Set of protocols created for the protection of packets at the network layer or lower
  - The function of higher level protocols such as TCP, UDP, ICMP, etc. are not affected
  - The benefits that this service provides are: access control, connectionless integrity, traffic-flow confidentiality, protection against replay packets, etc.
- Operates in two modes: Transport or Tunnel mode

IPSec cont.

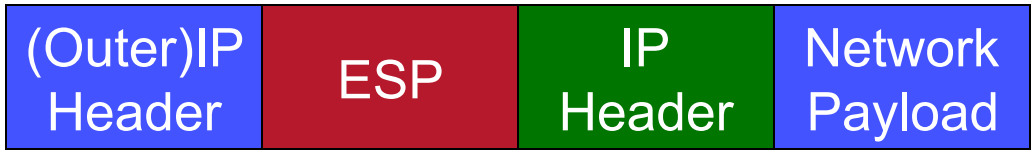
- Tunnel mode provides encryption of the data being sent as well as the source and destination IP address and all other header data

- Transport mode provides the protection of the data that is being sent

Security Associations

- SAs form the basis for IPSec
  - contract between two communicating entities
  - determine the protocols used for securing packets
- SAs are one-way, i.e. simplex
  - If two hosts are communicating, host A will have an SAout and an SAin
- SAs are protocol specific
  - Each host builds a separate SA for AH and ESP
- Security policy database
  - Works in conjunction with the security association database
- Security Parameter Index
  - 32-bit entity that is used to uniquely identify an SA at the receiver
  - SPI passed to AH and ESP headers using a tuple <spi,dst,protocol>

IPSec in Tunnel Mode

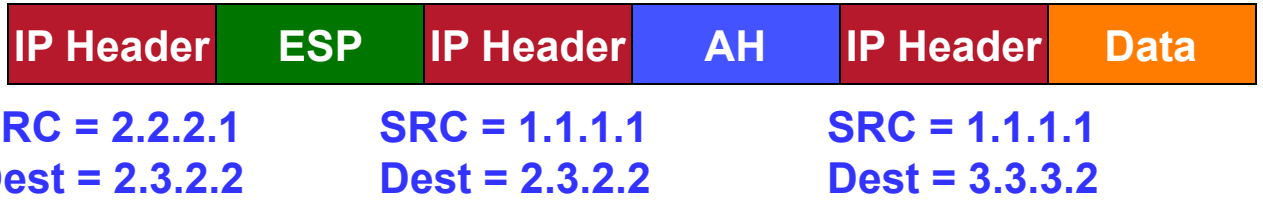


IPSec tunneled mode packet format

- **An IPSec tunnel mode packet has two headers – inner and outer**
  - **Inner header constructed by the host**
  - **Outer header is added by the device providing security services**

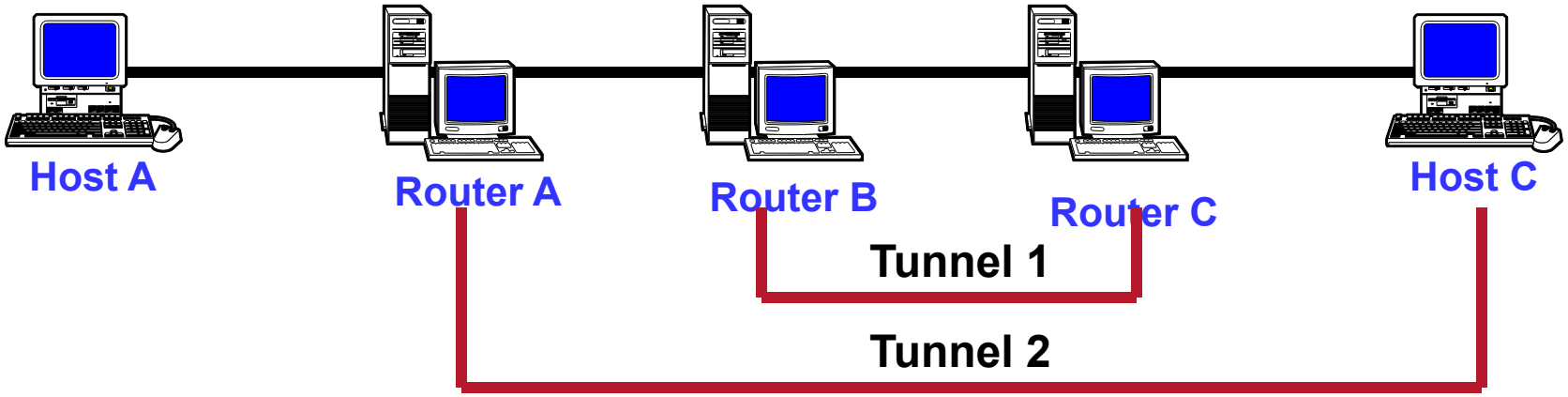
Nested Tunnels

Nested Packet Format

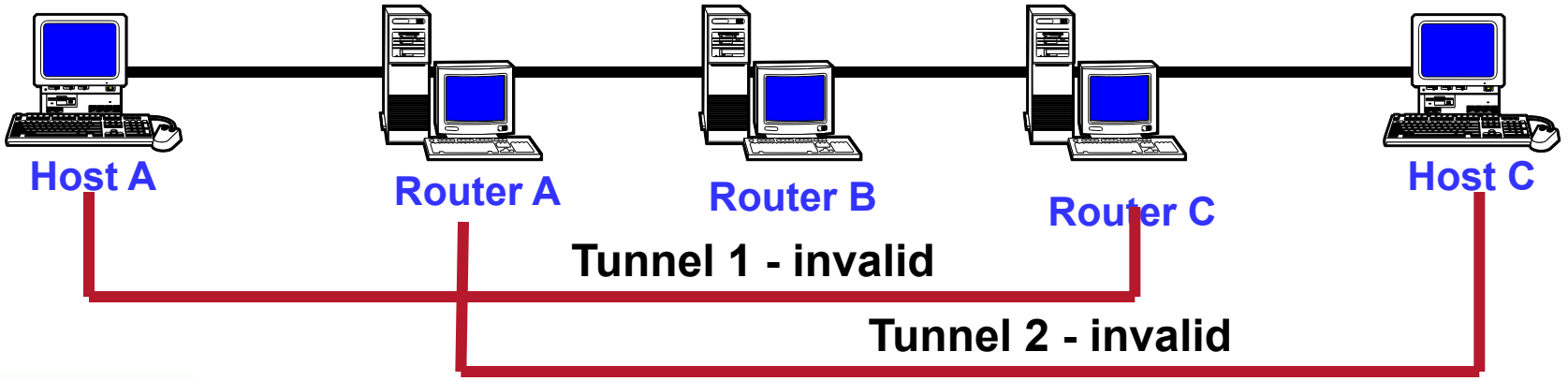


- IPSec defines tunnel mode for both ESP and AH
- In the nested tunnel example above, host A is sending a packet to host B.
  - Policy requires authentication to router B
  - VPN between the two networks bounded by router A and router B

Valid and Invalid Nested Tunnels

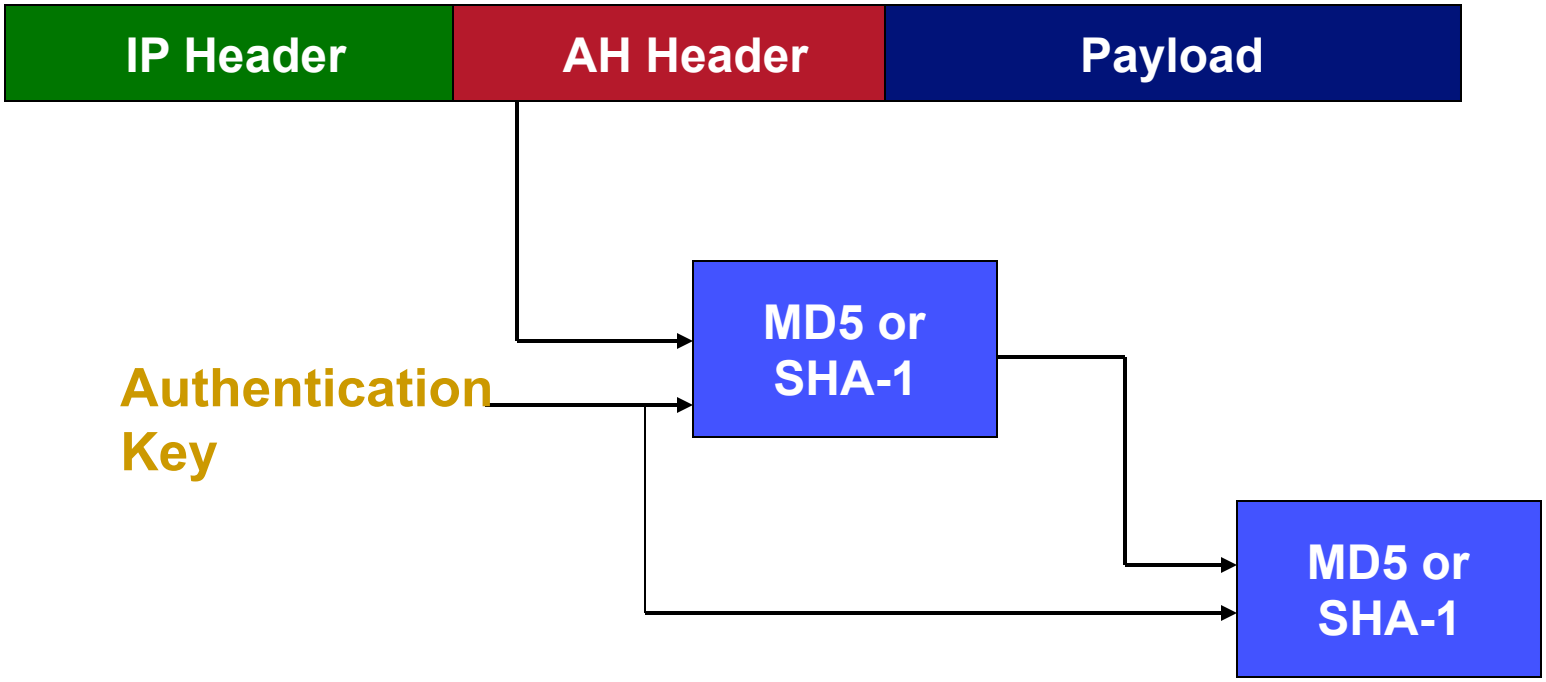


- The requirement for the tunnel is that the inner header must be completely encompassed by the outer header.



Authentication Header

1st 96 bits of second hash becomes Integrity Check Value (ICV)

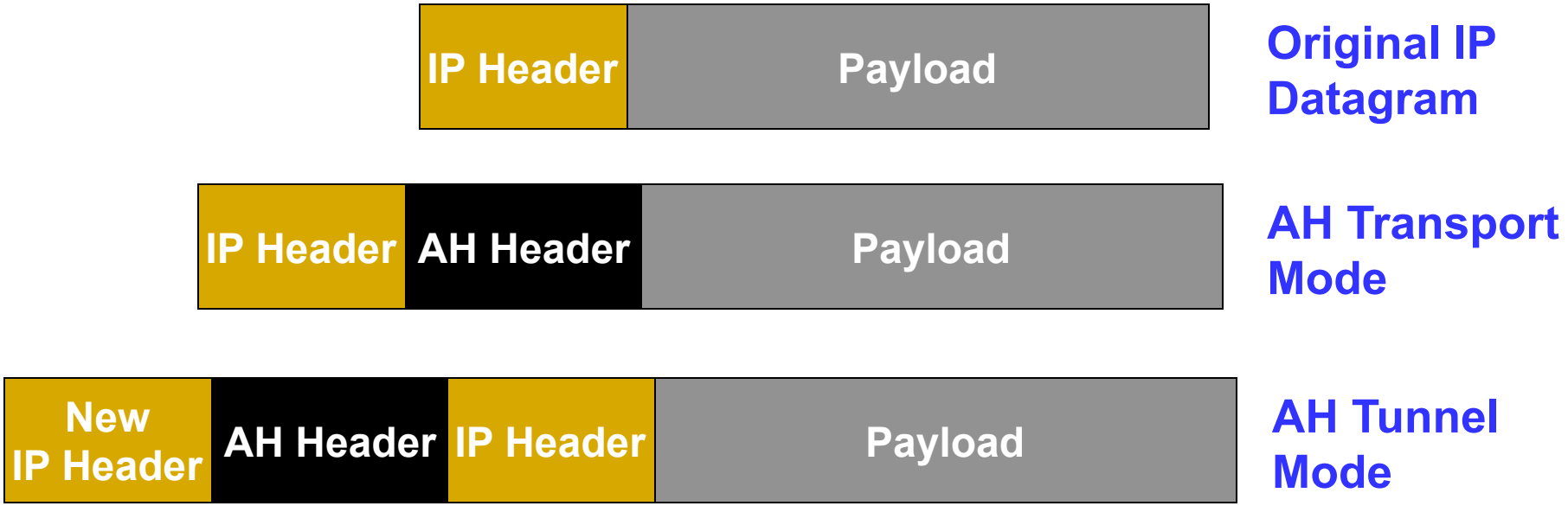


- 96 bits is selected to maintain compatibility with original IPSec spec
- Replay protection is provided by using the Sequence Number field within the AH header whose value is covered by the authentication procedure

Mutable IPv4 fields that cannot be protected by AH

- Mutable IPv4 fields that cannot be protected by AH
  - Type of Service (TOS)
  - Flags
  - Fragment Offset
  - Time to Live (TTL)
  - Header Checksum
- When protection of these fields is required, tunneling should be used
- Payloads of an IP packet are considered immutable and therefore always protected by AH
- An IP packet with AH applied can be fragmented but AH cannot be applied to a fragmented packet

AH Transport and Tunnel Modes



- In transport mode, the original datagram's IP header is the outermost IP header
- In tunnel mode, a new IP header is generated for use as the outer IP header of the resulting datagram
  - Source and destination address of the new header will generally differ – i.e. the destination address of the new IP header may be a corporate firewall.

Encapsulating Security Payload (ESP)

- ESP adds approximately 24 bytes per packet
- For interoperability purposes, mandatory to implement algorithms has been defined for ESP
  - The must-implemented cipher is DES-CBC with an explicit IV (RFC 2405)
  - The must-implement authenticators are HMAC-MD5-96 and HMAC-SHA-96 (RFCs 2403 AND 2404)
- Published prior to development of "deep crack"
- RFCs updated to indicate deprecated nature of DES and suggesting stronger cipher algorithms

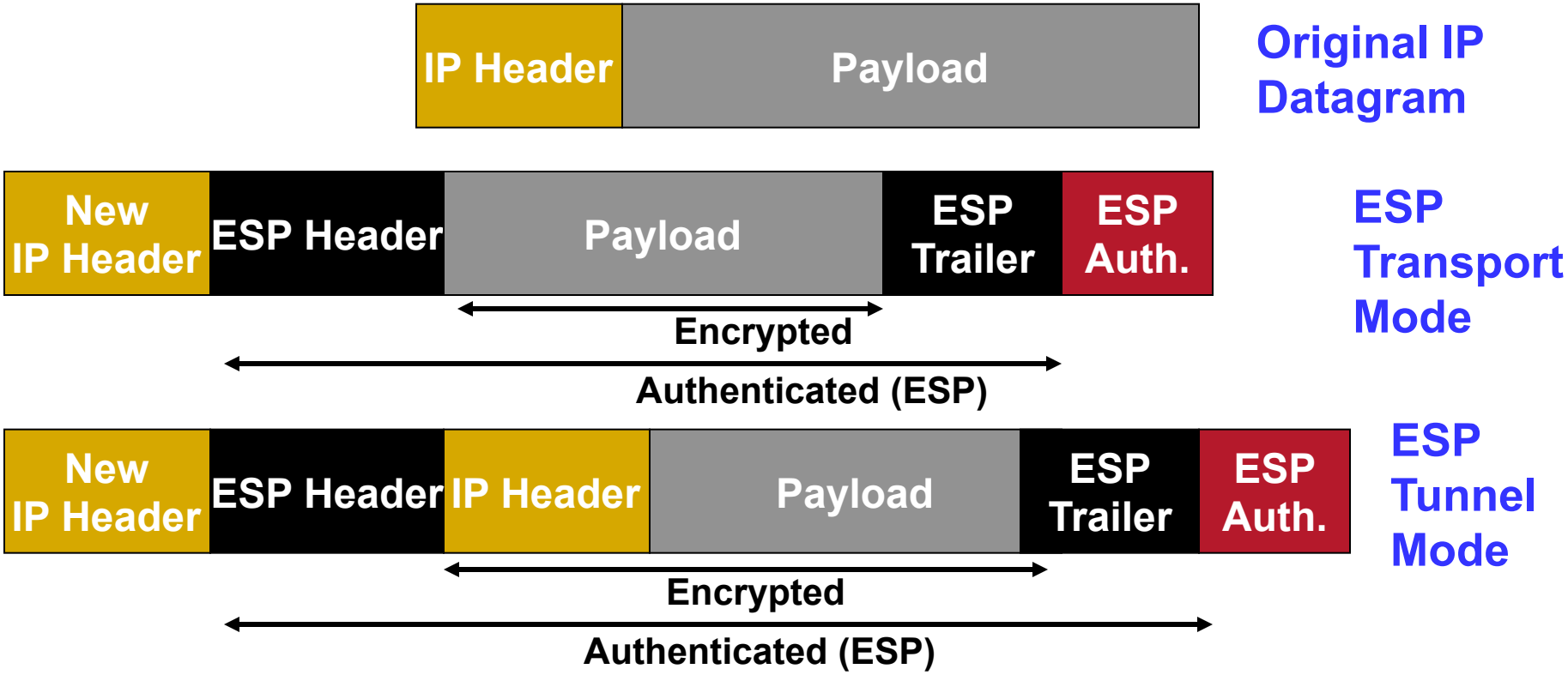
Outbound ESP Processing

- Insert header (similar for both IPv4 and IPv6)
- Encrypt packet from beginning of the payload to the next header field in the trailer using appropriate cipher specified in the SA (policy check)
- Authenticate packet from ESP header through the ciphertext to the ESP trailer.
  - Insert result in the authentication data field of the ESP trailer
- Recompute checksum of the IP header that precedes the ESP header

Inbound ESP Processing

- SA determines what the incoming packet should be.
  - No way to tell until packet is decrypted
  - Makes unauthorized traffic analysis harder
  - If no valid SA exists – drop the packet
- Next, authenticate by checking the message digest
  - pass appropriate key to authentication algorithm from the SA
- Decrypt the packet -- from the beginning of the payload data to the next header field
  - decrypted using the key and cipher algorithm from the SA
  - check decryption by checking the padding
    - padding is completely deterministic
    - verifies whether packet was successfully decrypted.

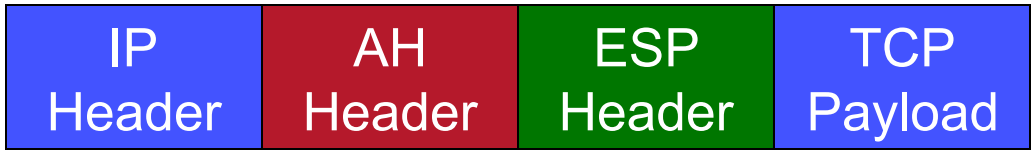
ESP Transport and Tunnel Modes



- ESP in transport mode provides neither authentication nor encryption for the IP header.
- In tunnel mode, the new IP header is not encrypted – everything else is

Transport Mode

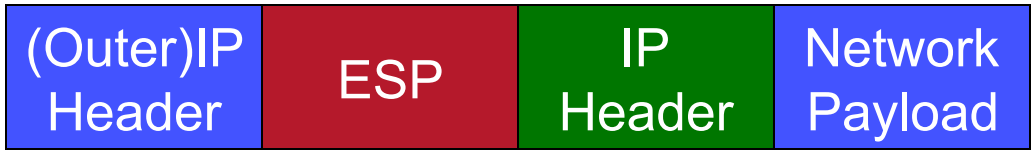
- **AH and ESP intercept the packets moving from the transport layer into the network layer.**
  - **When security is NOT enabled, TCP and UDP flow into IP which adds an IP header**
  - **When security is enabled, TCP / UDP flow into the IPSec component**
  - **When both AH and ESP are used, ESP is applied first – why?**



Packet format with AH and ESP

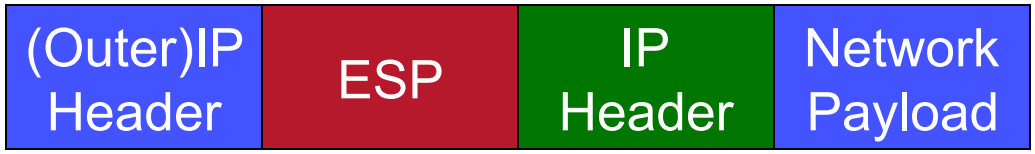
Tunnel Mode

- **IPSec in Tunnel mode is normally used when the ultimate destination of the packet is different from the security termination point.**
  - **ex. security termination point may be a router rather than a host.**
  - **also used when a router provides security services for packets it is forwarding**
  - **In the case of tunnel mode, IPSec encapsulates an IP packet with IPSec headers and adds an outer IP header**



IPSec tunneled mode packet format

IPSec in Tunnel Mode



IPSec tunneled mode packet format

- **An IPSec tunnel mode packet has two headers – inner and outer**
  - **Inner header constructed by the host**
  - **Outer header is added by the device providing security services**

AH vs ESP

- AH ensures integrity of the data
- ESP provides confidentiality of the data
- To make sure privacy and integrity is provided you can use both options

IPsec Key Management

- **IPsec support 3 methods for key management and exchange**
  - **Internet Security Association and Key Management Protocol (ISAKMP)**
  - **Oakley**
  - **Secure Key Exchange Mechanism for Internet (SKEMI)**

IPsec Key Management cont.

- IPSec provides the following abilities
  - Ability to change keys over a public networks using Diffie-Hellman key exchange
  - Public key signing of Diffie-Hellman key exchange to guarantee identity and avoid man-in-the-middle attacks
  - IDEA and 3DES for bulk encryption
  - HMAC, MD5, and SHA-1 for integrity checks
  - Digital certificates to act as digital ID cards between parties

IPsec Key Management cont..

- IPsec provides both manual and automated key distribution

- IKE (Internet Key Management) - provides automated process of key exchange
  - Security association negotiation occurs by creating a secure channel between two peers and then agreeing to terms across this channel
  - This is done over two phase. The first phase creates the channel and the next phase establishing the security association

Split Tunnel vs Full Tunnel VPNs

- **Split tunnel is a form of VPN where not all traffic is routed via the VPN**
  - **Split tunnel provides a performance advantage**
  - **Also opens the door to potential security vulnerabilities that could affect the information that was sent over the secure channel**

- **Full tunnel routes all traffic over the VPN**

TLS (Transport Layer Security)

- Successor to SSL
- Can be used to exchange keys and create a secure connection across a public network
- Has an advantage over IPSec based VPN in that it can more easily handle when networks are very heavily NAT encoded
  - IPsec can have issues crossing multiple domains

Always-on VPN

- Strategy to help users to always use secure connections
- Uses automation to connect to the VPN whenever an Internet connection is detected
- Tries to remove the obstacle of always having to enter credentials each time you want a secure connection

NIPS/NIDS

- **Network-based intrusion detection systems**
  - **Designed to detect, log, and respond to unauthorized network or host use**
- **Network based intrusion prevention systems**
  - **Has at its core an intrusion detection system**

NIPS/NIDS cont.

- In comparing the two:
  - NIDS provides alerts for what is seen as bad
  - NIPS performs actions on these alerts
  - NIPS has a NID as a component within it
  - NIDS detect, log, and alert on unauthorized network activity in real time
  - NIPS can take specific actions such as resetting or disabling connections

NIDS Components

- These are often implemented in software and have some core components, regardless of the vendor:
  - Traffic collector (sensor) - Responsible for actively monitoring logs or traffic entering or leaving a specific system.
  - Analysis engine - This is the brain of the system that checks data against a known signature database
  - Signature database - A collection of malicious patterns that highlight possible malicious activity
  - User interface and reporting - Provides the ability for an analyst to interact with the reporting system

NIDS/NIPS Types

- Alarms can be customized based on what system is being monitored
  - Would not want Windows alerts on a Linux system
- NIDS signatures come in a three primary forms
  - Signature-based
  - Heuristic/Behavioral
  - Anomaly

Signature-based

- Static strings that indicate particular behavior
- Has to know what is malicious beforehand to detect it
- Constantly requires updating to discover new attacks

Heuristic/Behavioral based

- **Behavioral**
  - Relies on a known set of “normal behavior” and highlights things that go against that behavior
  - Can find zero-day attacks
  - Can also be prone to high false-positive rate because traffic not seen before will be marked as malicious

- **Heuristic**
  - Uses artificial intelligence (AI) to detect intrusions and malicious traffic
  - Adds more flexibility and understanding to security alerts

Anomaly-based

- Similar to behavioral detection
- Taught what is normal and then looks for deviations from those patterns
- These are implemented using an artificial intelligence engine

Inline vs Passive Monitoring

- NIDS/NIPS have two options for studying and making decision on data
- Inline method looks at the actually data being sent and makes decisions based on these items
  - If there is a failure in a device that monitors the actual traffic then this blocks the traffic flow
  - NIPS devices can use this method to act as a gateway for what gets in and out
- Passive monitoring takes a copy of the data that is passing over the wire (sniffing the data)
  - Most devices perform passive monitoring

In-band vs Out-of-Band

- Very similar to the inline vs passive description
- In-band NIDS/NIPS are connected to an inline sensor and can make decisions on traffic from the actual sensor
  - This is beneficial for high value devices that will be accepting a very low number of traffic types
  - An example would be applying this in front of a corporate database that will only be allowing access via database connections

In-band vs Out-of-Band cont.

- **Out-of-band use passive sensors and have greater flexibility in what types of attacks that can be detected**
  - **The disadvantage is not being able to stop attacks directly**
  - **With this type of monitoring, traffic has already entered the network once alerted**

In-band vs Out-of-Band cont.

- **Out-of-band use passive sensors and have greater flexibility in what types of attacks that can be detected**
  - **The disadvantage is not being able to stop attacks directly**
  - **With this type of monitoring, traffic has already entered the network once alerted**

Rules

- Rules enable the NIDS/NIPS to perform the actions that they need to
- Rules can be simple, snort rules, or complex when it comes to heuristic/behavioral or anomaly-based systems
- In the future rules will be determined by utilizing analytics to make smarter decisions
  - NIDS/NIPS can be used to collect data to make the decision making process better

Routers

- Backbones of the Internet moving packets from one network to another
- Network management devices used to connect different segments of networks
- Use algorithms and routing tables to decide which paths are most efficient for delivering packets

Routers cont.

- Make sure to maintain security of routers by changing default password and administrative information
  - Also keep the router physically secure

- Routers are available from wide variety of venders and help to manage the infrastructure of companies around the world

ACLs (Access Control Lists)

- Used to manage if packets will be permitted to enter a network
  - Examines the source address to determine if a packet should pass
- Routers with built in ACLs can drop packets as described in the ACL
- Larger ACLs can negatively impact the performance of a router

ACLs (Access Control Lists) cont.

- Some routers can even act like they were application gateways and perform stateful inspection of packets as well as ACL checks

Antispoofing

- Used to help identify fraudulent packets being sent over the network
- One way for edge routers to do this is to perform source address checking
  - This makes sure that the sender's source address matches the packets that are being sent

Switch

- Today is the most common tool for Ethernet-Based LANs
- Have largely replaced hubs and bridges
- Provides an extra layer of security with the ability of a sniffer being able to see network traffic being greatly reduced
- Also drastically reduces the opportunities for collisions

Switch cont.

- Weakness of switches
  - Susceptibility to be greatly compromised if hacked
  - Some devices use Telnet and SNMP (Simple Network Management Protocol) for administration that are known to send passwords in cleartext
  - A hacker that gains access could go virtually undetected
- SSH should be the choice for configuring these devices
- Common suggestion is to disable all communication methods for a switch other than the secure options

Port Security

- This a functionality that switches provide that use the MAC address of devices to enforce security

- Switch can determine how many and which devices should be able to connect to a port based on their MAC address

Port Security cont.

- There are three versions of Port security
  - Static learning
    - Specific MAC addresses are assigned directly to ports
  - Dynamic learning
    - Allows the switch to learn MAC addresses once they connect
  - Sticky learning
    - Allows multiple devices to use the same port and has a security feature which stores information in memory to survive reboots

Layer 2 vs Layer 3

- Switches operate at the data link layer of the OSI model while routers act at the network layer
- For intranets switches are very important and serve a similar role that router do on the Internet
- Switches have become the primary network connectivity device, additional functionality has been added to them
  - There are some switches that can operate at the network level and provide some routing abilities, but they primarily work at Layer 2

Loop Prevention

- Switches operate at layer 2 of the OSI model, which has no count down mechanism to kill packets that get caught in loops or on paths that will never resolve

- Switches try to avoid the possibility of encountering loops by using spanning trees

- Spanning Tree Protocol (STP) provides multiple redundant paths, while breaking loops to ensure a proper broadcast pattern

Flood Guard

- There are a number of different flooding attacks that are possible
  - Ping flood, SYN floods, ICMP floods, and traffic flooding
  - Detecting a flood is very different from actively managing one
  - Floods are controlled by either dropping connections or managing traffic
- Flood guard manages traffic rate and percentage of bandwidth occupied by broadcast, multicast, and unicast traffic
  - Commonly implemented in IDS/IPS systems to prevent DoS and DDoS attacks

Proxy

- Used as a mechanism to manage and filter undesirable traffic and prevent employees from accessing potential malicious sites
- Proxy takes requests from a client system and forwards them on to a destination server
- Proxies are especially beneficial from a security perspective because they can control the types of outbound connections that users are able to make and limit the type of content they can access

Types of proxies

- There are a number of different types of proxies with some having different characteristics as well
- Transparent proxies require no user action to perform its responsibilities
  - Can modify a client's request before it is sent, and could even serve a request without communicating with the destination server
- Proxies can be setup for one specific purpose or can be multipurpose

Types of proxies cont.

- **Anonymizing proxy**
  - Can hide the identify of users from entities that track browsers cookies
- **Caching Proxy**
  - Saves a copy of content to preserve bandwidth and fill requests more quickly
    - Often used for larger organizations where employees could be viewing the same content and can be served quickly

Types of proxies cont..

- **Content-filter Proxy**
  - Often use at school, organizations, and government networks. Requests are compared to acceptable use policies to determine if they will be served or not
- **Open proxy**
  - Use to hide identify
  - Great for privacy advocates and bad for groups such as law enforcement
- **Web proxy**
  - Used as a web cache and to handle web traffic

Load Balancers

- Used to add a layer of fault tolerance on critical systems
- Spreads work out across two or more systems to help utilize resources better
  - The goal is not to overload any individual servers
  - If one system fails, the others can pick up the processing it was handling
- This device works by performing health checks to identify which machines are operating and uses a scheduler to spread work evenly

Scheduler

- **Algorithm that determines how tasks will be shared across systems**
  - **Two major options:**
    - **Affinity**
      - **This type of scheduling will send traffic from a specific host to that server for the duration of a communication**
    - **Round-Robin**
      - **Option 1**
        - » **Equally shares the amount of tasks that all systems will receive regardless of previous load**
      - **Option 2**
        - » **Uses a weighted variable that will be added to help better balance servers that are dealing with a few connections, but very large wait times**

More on Load Balancers

- To handle the load balancing well, you need multiple LBs to avoid the problems of having a single point of failure

- Schemes for multiple LBs
  - Active-Passive
    - Use a primary LB with a passive LB monitoring the health of the active device
    - If the primary fails, then the passive device will take its place
  - Active-Active
    - All LBs are active sharing the duties together

Access Point

- Devices used to govern the entry and exit of radio-based network signals into and out of a network
- Each AP will have a SSID (Service Set Identifier) that is the name for the AP
- A sign that the AP has not been configured for security is searching for common AP names and using default passwords for given vendors
  - Make sure that a unique SSID is used and the password is changed to something secure

Access Point cont.

- Another recommendation is to disable the beacon function of an AP
  - Will not see any advertisement beacons to connect
  - If a sniffer is used, the packets can still be discovered and the SSID determined

MAC Filtering

- The practice of filtering who has access to resources based on a known list of MAC address

- Can be applied to a number of different devices
  - Switches
  - Wired Networks
    - Good to use because you don't have to worry about spoofed packets
  - Wireless AP
    - Attackers can still watch to see which packets are admitted through and then determine the valid MAC addresses for spoofing

Signal Strength

- **Directly correlated to how usable a wireless signal is**
  - **To weak of a signal can result is dropped packets**
- **Can be affected by the transmitting power of a device and the environment in which transmissions are made**
  - **Significant metal in walls and roofs can weaken signals**

Signal Strength cont.

- **Adjustments in power level may be needed depending on the situation**
  - **Lower power levels will reduce the opportunity for interference but can also limit the range of signal strength**

Band Selection / Width

- **Multiple bands employed, with different bandwidths**

- **Wi-Fi can operate over two different frequencies, 2.4 GHz for 802.11 b/g and n, and 5 GHz for 802.11 a,n, and ac**

Antenna Types and Placement

- **Wi-Fi uses antennas to transmit and receive signals over the radio based communication method**

- **Placement and design can play a major role on usability**

Antenna Types and Placement cont.

- Antennas come with different transmission types and gain factors
  - Gain is a measurement of antenna efficiency
  - Antennas with higher gain can find weaker signals, but have a more limited range
  - Wide coverage antennas can cover a wider areas, but with lower gain factors.

- For complex buildings this often calls for the need of a site survey to determine the proper placement of APs

Antenna Types and Placement cont..

- **If signal strength issues arise, changing the antennas used can provide a boost**
  - **Depending on how the signal is improved, the type of antenna you choose is important in not allowing your signal to bleed outside of the building**
  - **Choosing directional antennas are helpful**

Fat vs. APs

- **Fat APs are devices that perform a number of different actions itself**
  - **Authentication, encryption, and sometimes channel management**
  - **They are called fat or thick based on the amount of work the AP is required to do**

- **Thin APs allow for centralized management and control**
  - **These are often better for larger organizations**
  - **Allow for better load balancing, deployment of patches and firmware updates**

Fat vs Thin APs

- **Allow for the use of Network Access Control where users are placed in groups that have specific sets of acceptable resource utilization**

Security Information and Event Management (SIEM)

- **Security Information and Event Management**
  - **Systems that compose both hardware and software used to classify and understand what security data means**
- **Collects data from a number of different sources**
- **Wide range of vendor options going from free to very expensive**

SIEM - Aggregation

- Collecting information from a number of different sources into a common format
  - Data is placed in a centralized location for analysis and decision making

- Data sources can include system event logs, firewall logs, security application logs, and other programs that feed information into security appliances

SIEM- Correlation

- Finding the relationships between many different types of events to develop some type of intelligence
- Can be used to find patterns of events for a final action to be taken
  - Noticing port scanning from an outside IP address could make it suspicious and future actions from that IP can be marked as suspicious
  - Can provide earlier warnings from data collected before malicious activities occur
- Correlations can be based on time, behaviors, common events, etc.

SIEM- Alerting and Triggers

- **Have the ability to identify specific predetermined patterns and either issue alerts or react to them**
  - **Use rules and analytical engines to perform these actions**
- **SIEMs can be considered a much more powerful IDS**
  - **Can use external information as well as traffic information to make decisions**

SIEM- Time Synchronization

- When working with enterprises that are globally dispersed a method of correlating events specific to their own time zone as well as globally is required

- SIEMs allow for the reading of both types of timing information simultaneously
  - Local Time
  - UTC (Coordinated Universal Time)
    - Global time standard
    - Essentially a global time zone

SIEM- Event Deduplication

- When collecting data you can have multiple data sources that can report the same instance of events
- Saving these duplicate forms of information can skew results and analytics
- SIEMs provide an ability to identify event duplication and remove them from the data
- This requires a centralized storage location for SIEM data to perform this correlation and removal process

SIEM- Logs/WORM

- Logging information comes from a number of different sources and are placed in a standardized format
- SIEMs can use database tools that take this data and molds it into informative reports
- SIEMs adhere to the WORM principle of “write once, read many” to be more operationally efficient
  - This helps when working with very large data sets and an abundance of information

Data Loss Prevention (DLP)

- Technology is responsible for monitoring user activity and making sure no sensitive information is released
  - Can include strings such as account number, social security numbers, or specific files
- If certain characteristics are found in data in transit, then the transfer can be blocked
- Important aspect of using a DLP device is the placement of the device
  - Needs to be able to see the actual data to be effective
  - Encryption procedures thwarts its effectiveness

DLP – USB Blocking

- USB provides a way for data to be exfiltrated from a system very easily
- USB blocking can be used to protect against this security threat
  - Either disabling physically or through software the use of USB devices
- From a software perspective, the use of USB ports could be limited by requiring access codes to perform transfers

DLP- Cloud-Based

- Cloud technology allows for the storage of very large datasets and the freedom to access the information from anywhere
- These cause problems for DLP systems
- Vendors have developed solutions to manage these issues while still allowing customers to have control over their data transfers

DLP- Email

- Email is one of the most common forms of communication in enterprise environments
  - Files are normally attached to email messages
  - This is a venue for exposing information

- DLP devices can connect to mail servers to make sure that no sensitive information or files are being transferred

Network Access Control (NAC)

- Managing networks of connected devices can rise a number of different issues, including the types of software running on the connected devices
  - Just having a secure network does not mitigate potential problems from devices using the network
- NAC refers to managing endpoints on a case by case basis as they connect to a network
- Two competing technologies are Network Access Protection (NAP) and Network Admission Control (NAC)

Network Access Control (NAC) cont.

- NAP is a Microsoft technology that manages network access to a computer host
- NAC is a Cisco technology for controlling network admission
- NAP aims to measure the health of the system attempting to connect a network

NAC- Dissolvable vs Permanent

- NAC technology requires checking the state of systems before they connect to a network
  - This is done with agents that are responsible for performing these checks
  - Dissolvable agents are deployed as needed while permanent agents act as the gateway to NAC functionality

NAC- Host Health Checks

- **Many parameters can be used to evaluate the health of a system**
  - **Is AV present?**
  - **When was the AV last run?**
  - **Does the system have the latest patches for the OS and applications being used?**

- **If constraints aren't met**
  - **Access can be denied completely**
  - **System is required to fix health concerns before granting access**
  - **System is placed on an isolated network segment**

NAC- Agent vs Agentless

- Since deploying agents to machines can be problematic, vendors have developed agentless solutions

- Rather than reside on the machine, agents can operate from within the network
  - Agents have persistent code running on a host
  - Agentless the code resides on the network and is deployed in memory when a request to connect is made

Mail Gateway

- This device is optimized with hardware and software to process e-mail packets on a network and provides a wide range of e-mail-related services
  - Filtering spam
  - Performing encryption
  - Etc.

Mail Gateway- Spam Filtering

- **Spam**
  - Any type of unsolicited message via email, text message on mobile devices, or any type of random posting
- **Spam filter**
  - Software designed to remove spam from an email stream
- **Spam protection methods**
  - Blacklisting
    - Blocking a known set of domains that have been used for spamming in the past

Mail Gateway- Spam Filtering cont.

- **Content or keyword filtering**
  - Looking for certain terms or phrases that could be indicators of spam
  - This method could lead to a number of false positives because some words can be used in both spam and legitimate messages
- **Trusted Servers**
  - The opposite of blacklisting, only accepting messages from those whom you trust
- **Delay-based filtering**
  - Method used to identify spammers that bombard SMTP servers as soon as a connection is started
    - If messages are sent before an SMTP welcome message is created, those systems are considered to be spam generators

Mail Gateway- Spam Filtering cont..

- PTR and reverse DNS checks
  - Checks the origin domain of the e-mail sender for the criteria that most spammer have:
    - Dial-up user
    - Home-based broadband
    - Dynamically assigned address
    - Missing or generic domain
- Callback verification
  - Check to make sure the sender of spam messages have not been spoofed
    - This check may not be a good indicator because some spam messages come from legitimate sources

Mail Gateway- Spam Filtering cont...

- **Statistical content filtering**
  - Uses a system learning based approach where users help to identify what is spam and what is not
  - The system learns from the characteristics of the messages that have been provided a label
  - Some spammer place additional content in the messages to intentionally cloud the learning ability of the system
- **Rule-based filtering**
  - Look for common keywords and content in certain fields that can be used to block messages
- **Egress filtering**
  - Utilizes the methods already discussed and just applies them to messages leaving an organization's network
  - Aims to identify any resources that have been taken over to be a spam generator

Mail Gateway- Spam Filtering cont....

- Hybrid filtering
  - Uses a combination of some/all of the methods discussed previously to protect against spam

- Spam filtering tools and mechanisms are normally centrally placed to monitor incoming and outgoing messages
  - This is normally at the network or SMTP server level

- Spam filters have gotten better, but spam will continue to be a pervasive problem

Mail Gateway- Data Loss Protection

- DLP is an issue for outgoing mail as stated previously

- Two solutions are normally available:
  - Have standalone system that is responsible for scanning the attachments of outgoing email
  - Use an integrated DLP solution that scans both outgoing traffic as well as e-mail.
    - An advantage of using an integrated system is that it requires only one list of keywords to manage

Mail Gateway- Encryption

- Email is a plain-text protocol which makes it susceptible to eavesdropping anywhere between sender and receiver
- Email encryption can protect e-mail from eavesdropping as well as add authentication services

Mail Gateway- Encryption cont.

- **Problems have come with finding a standard protocol that will be able to be supported on all systems**
  - **Enterprise solutions have been created, but there is still difficulty in managing challenges for standalone external users**

Bridge

- Device used to perform network segmentation
  - Operates at layer 2 of the OSI model
  - A benefit to network segmentation is the security it provides
    - It helps minimize the distance that sensitive data has to travel and keeps that information in only the area that it belongs to reduce exposure
- Networks can be segmented using bridges, switches, and VLANs.

SSL/TLS Accelerators

- Process of encrypting traffic per SSL/TLS protocol is computationally expensive
- Used to alleviate the encryption bottleneck for large-scale web servers
- Hardware device that sits transparently between the web server and the Internet

SSL Decryptors

- Are used to monitor traffic entering and leaving networks
  - Helps solve the problem of inspecting data that has already been encrypted before leaving the network
- Can selectively decrypt and check the contents of traffic and then re-encrypt once the analysis is complete
- Performs the equivalent of a man-in-the-middle method for the inspection of traffic

Media Gateway

- Devices used to handle the heavy demand from digital media channels
- Used to translate information from one protocol to another
- Can be a standalone device or be integrated into a switch/firewall

Hardware Security Module (HSM)

- Device used to manage the storage of encryption keys
- Designed to provide efficient cryptographic operations, without disclosing keys
- Have tamper protection mechanisms to prevent physical access to the secrets keys they protect
- HSMs help to allow keys to be used without exposing information to potential host-based threats

Security Tools and Technologies
Technologies & Tools

Reference:

Drew Hamilton Lecture Notes

DeMarcus Thomas

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

Protocol Analyzer

- A very broad term that could include the monitoring of many different types of communication protocols
  - In this context most notably refers to network based analysis
- Can be used to capture wired or wireless traffic using hardware or software based tools

Protocol Analyzer cont.

- Have the ability to place its interface in promiscuous mode
  - Allows the tool to accept and process packets that it collects
    - Even if they are not destined for that particular system
- Can be used as a diagnostic tool to understand what type of traffic is being sent into or out of the network
- Must be well placed to make sure all traffic information is collected
- Good example of software based tool is Wireshark

Protocol Analyzer- SPAN

- **Switched Port Analyzer**
  - **This term is normally used by Cisco, while other vendors call it port mirroring or port monitoring**
- **The functionality is to be able to forward packets from a port on a switch to a dedicated port specifically for packet capture**
- **The data collected is fed into protocol analyzers or IDS/IPS**

Network Scanners

- These types of tools are essential for security professionals and attackers to map out and understand what is on a network
- Can be used to scan for live hosts, identify active ports, find services that are running on hosts, and determine TCP/UDP services
- Capable of running on any IP network
- The most common tool for this is Nmap

Network Scanners cont.

- As a security professional, you must be careful when conducting a network scan
  - Could activate an incident response activity
- In scanning a port, there are a number of different responses that can be returned
  - Open
    - Ports accept connections, but additional filtering could be occurring
    - Port can be reported open for the network scanner, but not accept any other connection
    - Example: port 22 can seem open, but then refuse any attempted SSH connections

Network Scanners cont..

- **Closed**
  - Normally the response when a system returns an RST packet
- **Filtered**
  - This response is typical when an ICMP unreachable error is returned
  - This could signal the port is being filtering by a firewall or some other device

Network Scanners cont…

- **Additional types**
  - **Depending on the network scanning tool, additional responses can be something similar to dropped, blocked, etc.**

- **To get a clear picture of a network's make up, use a number of different scans at different times of the day to get a clear picture of activities**

Network Scanners- Rogue System Detection

- In order to determine what is abnormal, you must know what is normal
  - Most security controls start with understanding the authorized hardware and software in an environment
- Rogue system checks can be done by active scanning a network for unauthorized devices
- Passive scanning can be performed to check what devices may established unauthorized communications

Network Scanner- Network Mapping

- This type of tool is another name for a network scanner
- Main goal is to develop an understanding of how a network is built, the types of nodes on the network, the OS they may be running, the purpose of the system, etc.
- Network analyzers are also network mappers, by definition

Wireless Scanner / Cracker

- These types of tools help to identify who is connecting to the wireless network, what is being accessed, and how those activities align with the security plan
- Common wireless scanning tools
  - Kismet
  - NetStumbler
  - MiniStumber
- Common wireless cracking tools
  - AirSnort
  - AirCrack
  - CoWPAtty

Password Crackers

- System administrators will want to use password crackers to verify that their systems don't have weak entry points
- These crackers use dictionary list and brute force to find weak passwords on a system
- Some password crackers can work online to attack a system, but normally subject to some type of timeout after too many tries
- Other tools will work directly on password files, if they can be obtained by an attacker

Vulnerability Scanner

- **Highly valuable in determining specific problems on a system that could be exploited**

- **Scanner comes in three general forms**
  - **Network Based**
    - **Commonly used to scan for vulnerabilities over the network**
    - **Helps you to perform a broad sweep vulnerability check on one or many devices**
    - **Example tool**
      - **Nessus (Tenable Network Security)**

Vulnerability Scanner cont.

- **Host Based**
  - Looks for vulnerabilities specific to a given system
  - Most host based analyzers must be running on the system being checked
  - Can check for vulnerabilities directly in the OS
    - Problems could be cause by problems such as unapplied security patches
  - Example tool
    - Microsoft Baseline Security Analyzer
- **Application Based**
  - Checks for problems specific to a software version or scans a particular type of software for vulnerabilities
  - Web application vulnerability scans have become popular
  - Example tool
    - Acunetix WVS (Web Vulnerability Scanner)

Configuration Compliance Scanner

- **Major need is present to automate configuration checks**
  - **This is addressed with the Security Content Automation Protocol (SCAP)**
- **Configuration compliance scanners can be use to inform system administrators of configuration issues based on predefined rules**
  - **Running the tool the first time can be used to set a baseline and future changes are validated against that baseline**

Exploitation Frameworks

- Tool set used to assist hackers and security professionals in tasks to exploit/identify vulnerabilities on a system
- Security professionals can use such a tool to assess the extent of a vulnerability's effects
- Common example of this type of tool is Metasploit

Data Sanitization Tools

- Tools focused on removing important information from a system
  - This could be for system retirement or disposal
- Tools can be used to wipe entire disks
  - Leaves all data unrecoverable
- Use self-encrypting disks
- Destroying the encryption key leaves disk unreadableTools can also be used to remove specific information
  - Tools such as Identity Finder can do this

Steganography Tools

- Steganography is the science of hidden writing, or the hiding of messages in other content
  - Hiding digital information in images, videos, or audio files
- If information is hidden from normal users, then it is considered steganography
- Same techniques are used to add watermarks to trace documents that are copied for potentially identifying information leaks

Honeypot

- Honeypot is a server designed to act like a real server on a corporate network, but contains no real data.
  - It is a trap to detect potential activities of attackers and protect against them
- Same concept applies to Honeynets, it is a network that has been made attractive to attackers

- These types of systems help to identify:
  - Where attacks are coming from
  - Who is performing the attack
  - Gives insight into the attack methods and targets

Backup Utilities

- Backs up data in case of loss
- Underrated, but extremely important task
  - Must segregate data
  - Manage the actual backup files
  - Make sure the solutions scale well
- This can be difficult when dealing with enterprise networks and requires reliable tools

Banner Grabbing

- Attempts by attackers to gain information about a system through the banners that systems display
  - Attacks could identify the following
    - Services by type
    - Version of software
    - Unresolved errors
    - Etc.

- Banners can display service specific information that attackers could use as an identification mechanism

Passive vs Active

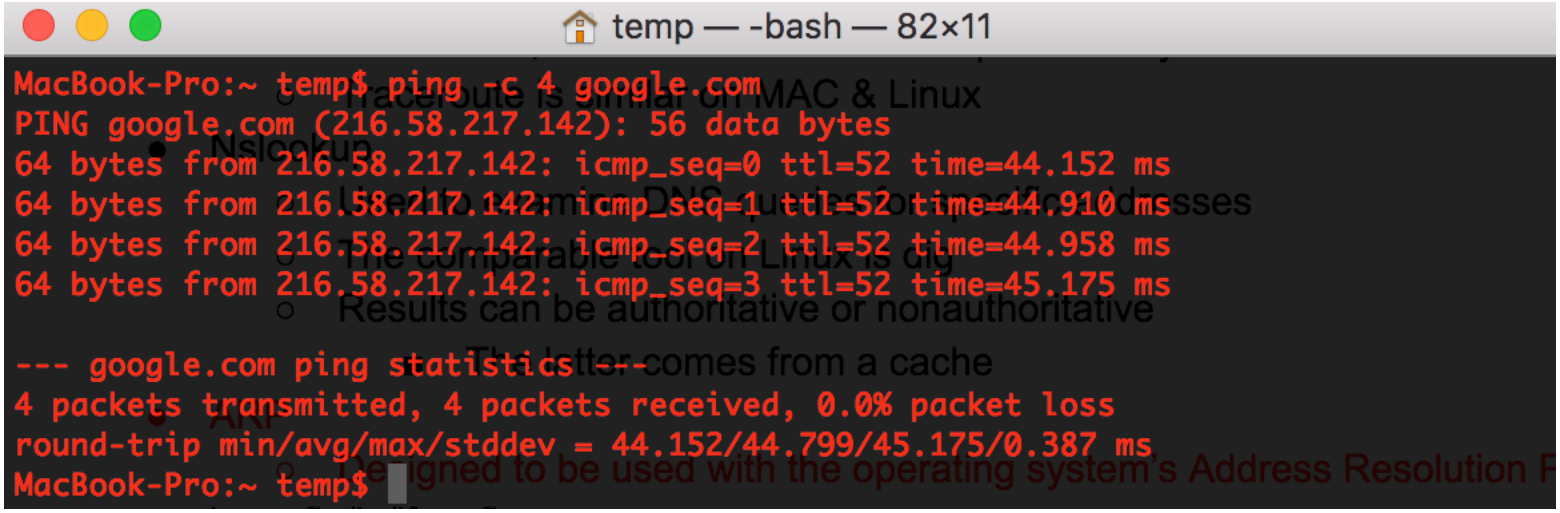
- Passive tools use existing traffic to perform analysis activities
- Active tools must interact with a target system and have the potential of its actions being detected
- Passive tools are more desirable to attackers when they have time to collect large amounts of information about systems
  - They have their drawbacks in that they must be placed between the source and the destination to be effective

Passive vs Active cont.

- Active tools don't have this requirement, but its actions can lead to being exposed
- Passive tools listen and receive, while active tools modify or send traffic

Command-line Tools

- **ping**
  - **Sends echo request to a designated machine to check if communication is possible**



Command-line Tools

- **netstat**
  - **Used to observe connections to and from a system**
  - **netstat –a Lists all active connections and listening ports**
  - **Netstat –at Lists all active TCP connections**
  - **netstat –an Lists all active UDP connections**

Command-line Tools

- **tracert**
  - **Traces the routes of packets over the Internet**
    - **Identifies the hosts, switches, and routers in the order that a packet passes by them**
  - **Uses ICMP, if blocked then does not provide any information**
  - **Traceroute is similar on MAC & Linux**

Command-line Tools

- nslookup
  - Used to examine DNS queries for specific addresses
  - The comparable tool on Linux is dig
  - Results can be authoritative or nonauthoritative
    - The latter comes from a cache

Command-line Tools

- arp
  - Designed to be used with the operating system's Address Resolution Protocol
  - Used to find information such as, where to send a packet using the MAC or layer 2 address

- Example queries
  - ARP request – "Who has this IP address"
  - ARP reply – "I have that IP address; my MAC address is .."
  - Reverse ARP request (RARP) - "Who has this MAC address"
  - RARP replay – " I have that MAC address; my IP address is …"

Command-line Tools

- ipconfig/ip/ifconfig
  - Ipconfig and ifconfig are tools for manipulating the interfaces on a system for Windows and Linux respectively
  - Can list interfaces, connection parameters, and refresh/ renew connections
  - ip command in Linux is used to show and manipulate routing, devices, policy routing, and tunnels
- tcpdump
  - Tool to analyze network packets
  - Can create pcap files and filter between input and output
    - This can be beneficial because of the large data load when analyzing network traffic

Command-line Tools

- nmap
  - Command to run nmap utility
  - Network scanner
  - Developed by Gordon Lyon and has been the standard network mapping utility for Windows and Linux since 1999
- netcat
  - Linux command-line tool with some Windows ports
  - Used to read from and write to TCP and UDP
  - Has redirection capability and can turn any process into a server

Security Technologies

- Number of different technologies that can be utilized to analyze security situations

- For the following technologies the goal is to be able to interpret the results from the following security tools to be able to address a security problem

HIDS/HIPS

- Host-based Intrusion Detection System and Host-based Intrusion Prevention System
- Alert on behavioral patterns that are matched
  - Depending on the sensitivity of the ruleset, a high number of false positives could arise
- HIDS are primarily a notifier while HIPS can take action
  - HIPS devices could send a reset signal to a device depending on the rules that are set breaking a potential malicious communication path

Antivirus

- Check applications for matches against known types of malware

- If a file is found to be malicious, there are two recommended actions
  - Quarantine the file
  - Erase the file using the AV utility

File Integrity Checker

- Tool used to check if a file is valid based on a previously calculated hash value

- For Windows, a system file integrity check can be performed with the following command
  - sfc /scannow

Host-Based Firewall

- These types of firewalls are tuned to that specific machine
  - Beneficial for systems such as high value servers
- If done correctly, this type of firewall will be tuned to have very low false positive rates and be able to block malicious connection attempts

Application Whitelisting

- Files that are marked safe to run based on their hash values
- For systems with a small number of applications, this can be a very effective mechanism
- For the Enterprise version of Windows, this can be done by using a tool called Applocker

Removable Media Control

- Removable media provides an attack vector for both data exfiltration and/or malware infection
  - Removable media controls aim to remediate these concerns

- One such control is based on an encryption-based method
  - As files are transferred, they are encrypted by a key that resides on the system
  - External drives can be used as a backup drives, but content will not be readable outside of the machine

Advanced Malware Tools

- Tools such as Yara are examples of advanced malware tools
- Yara finds patterns that malware leaves behind in memory which indicate that a system has been compromised
- Additional tools to note are threat prevention platforms
  - Analyze systems and traffic in real time
  - Alerts engineers of common malware artifacts such as callbacks to external devices

Patch Management Tools

- Tools used to help notify administrators and then pass this information on to users about when patches are available for the OS or applications on the system
- Some of these tools also have the capability to help apply patches
- These tools also can alert administrators when patches have not been installed in a timely manner

Unified Threat Management (UTM)

- All in one device that can offer a wide range of services
  - Switching
  - Firewall
  - IDS/IPS
  - Anti-malware
  - Anti-spam
  - Content Filtering
  - Etc.
- Normally designed for small to mid-sized networks to help simply security administration
- If alerts come from this type of system, it should trigger an incident response activity

Data Loss Protection (DLP)

- Technology designed to detect and prevent transfers of data across an enterprise
- Can scan packets for specific patterns, and if found can block the transfer
- The DLP must be placed where data can be observed, so if data is encrypted this method is thwarted

Data Execution Prevention (DEP)

- Protection of specific memory areas as non-executable in a Windows system
- Helps to protect against attackers changing the operation of a program through code injection into a data storage location and then executing the code
- If a DEP violation occurs, the OS will kill the program

Web Application Firewall (WAF)

- WAFs designed to perform restrictions based on rules associated with HTTP/HTTPS traffic
- This is a type of content filter and allows the capability to provide significant protections
- WAFs can be very granular in what is allowed and what is not
- Can also protect against the disclosure of critical data such as account numbers, credit card number, etc.

Troubleshooting Common Security Issues
Technologies & Tools

Reference:

Drew Hamilton Lecture Notes
DeMarcus Thomas

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

Troubleshooting Common Security Issues

- Troubleshooting common security issues is a skills that security professionals much constantly develop
- This section identifies security issues and provides methods for solving those issues

Unencrypted Credentials/Clear Text

- The transfer of credential information should never be transmitted in plain text
- This information is left vulnerable in two primary ways
  - The information can be seen by any machine that is in the communication path
  - The information could be saved in activity logs and be subject to discovery later
- To protect against unauthorized observations, this information should never been transmitted in an unencrypted form

Logs and Event Anomalies

- Only information that could be useful in identifying anomalous events should be logged
- A question to ask is if what is being logged could have a potential security implication
- If successful login information is missing when it should have been collected, this is an example of anomalous behavior
  - Additional events that could be a signal are users that normally log into a system monthly now logging in very late each night

Permission Issues

- These types of problems deal with users attempting to access or use resources
- This can be corrected by verifying user rights and permissions
  - Certain groups of people/employees will have certain rights to access information or activities
- A very good control is to periodically audit user rights to keep them up-to-date

Access Violations

- This involves the denial of using some resource due to improper permissions
- This happens for two reasons
  - Someone doesn't have permission and they are attempting to get around the security measures
  - The permissions for a person are set improperly
- For the latter, the user can then request for an update to their permissions

Access Violations cont.

- **Some malware can produce access violations as they probe for information**
  - **Keep track of information about these violations and information related to it**
  - **Security Information and Event Management (SIEM) devices can help highlight information that could be important**

Certificate Issues

- Certificates are used to carry public keys and help to vouch for a system's identity
- Certificates can be made invalid by having a trust chain that cannot be verified all the way back to a root node
- If an invalid certificate is installed into a trust repository, this could cause problems in the future with certificates that should not be trusted being trusted

Data Exfiltration

- This is an attempt by attackers to take data that resides on your system and transport it off without authorization

- There are a number of risk mitigation steps that can be taken to prevent this
  - Data minimization - only store data that is pertinent to business needs either now or in the future
  - Use DLP technology to prevent data from being exfiltrated in real time
  - Implement methods such as network segmentation and device such as firewalls to make data more difficult to access by attackers

Data Exfiltration cont.

- An additional option is to use options such as Bitlocker on USB drives
  - This encrypts information that is transmitted to a drive and leaves the key used to decrypt on the system.
  - The USB is now unreadable outside of the enterprise

Misconfigured Devices

- One of the most common security issues that can easily go unnoticed
- Many security controls work on the assumption that devices are configured properly
- Areas and devices where configuration is essential:
  - Firewalls, content filters, access points, etc.

Misconfigured Devices

- This misconfiguration issue is common enough that the NIST Risk Management Framework states specifically that controls must be tested once they are put in place to ensure they actually work as desired

Firewalls

- Devices to enforce network access policies
- Using a set of predefined rules, packets are either allowed or blocked passage
- Over some time rules can become messy due to needs for “temporary” exceptions for testing operations
  - These exceptions can be forgotten and then be targeted by attackers
- Auditing rules against organization policies can find these problems, but are expensive and time consuming
  - Auditors must then check to make sure that tests have been completed before exception rules are removed

Content Filter

- Used to limit specific types of content on the Internet to users
- Can also block sites that are non-work related and deemed inappropriate based on a set of rules
- Just like many other systems, the rule maintenance process can cause problems
- Common problem is rules that too broadly block content and hinders productivity

Access Points

- The first defense mechanism for who should be granted or denied access to a network
- The rules of an access point determine how effective it is, regardless of the overarching technologies that are using them
  - ACL
  - RADIUS (Remote Authentication Dial-In User Service)
  - Network Access Control (NAC)
- Rules must accurately describe who should have access to the network

Weak Security Configurations

- **Security configuration decisions that add avoidable levels of risk to software applications or operating systems**
  - **Example of this would be choosing out of date cryptography cipher suites to protect systems**
  - **Another example would be allowing unlimited login attempts as a policy when logging into a system**

Personnel Issues

- Problems that arise that are caused by the actions or errors of people who work for or in an organization
- Poorly trained people can make the most thought out security plans worthless quickly
- Employees have unknowingly released important company information via social engineering attacks
    - Operating system information
    - Policies and procedures
    - Supply chain information
    - Personnel records
    - Etc.

Policy Violation

- This happens when employees do not adhere to written policies established by the organization
  - This can stem from a number of different actions
    - Password violations
    - Acceptable use policies
    - Avoidance of rules via willful disobedience
    - Etc.
- All problems can be resolved by using training, other than the acts of willful disobedience

Insider Threat

- Opens the door for attacks from the inside
- A good example of this is Edward Snowden performing insider attacks at the NSA
- A way to protect against this is a defense in depth strategy
  - Use HR resources to gauge morale of new hires
  - The other is separation of duties
    - No one individual should have the ability to conduct transactions without some type of oversite or collaboration
  - Make sure admins do no have the ability to manipulate the logs on the systems they administer

Social Engineering

- Hacking a user/employee through misdirection and manipulation
- Manipulating users to provide information or perform actions that could be an advantage to the enemy
- To combat this provide your employees with comprehensive training to highlight some of the tactics for social engineering

Personal E-mail

- Using personal e-mail at work could cause a data exfiltration infraction that is outside of corporate control
- This can also be a pathway for attackers to introduce malware
- Many companies prohibit the use of personal e-mail in the workplace

Unauthorized Software

- Knowing the authorized software and hardware in a company greatly increases its security posture
- Adding undocumented or unapproved software can introduce additional attack surfaces for malicious actors
- This can be avoided by removing the user's ability to add software to systems
- Deep freeze software can also be used to reset systems to a known state once a user logs out

Baselining

- Measure of a system's current state of security readiness
- This method works by setting up the desired system with weaknesses addressed as a baseline, and then comparing future changes to this baseline to see what has changed
  - If changes introduce new risk, then evaluate those risks to mitigate them
- Largest problem is running the baseline scans, or automating them, to determine when deviations occur

License Compliance Violation (Availability/ Integrity)

- Software license violations can result in the inability to use software
- Software in an improper license state may not receive proper updates
- These issues should be corrected quickly to avoid not having software available when necessary

Asset Management

- One of the top 20 common security controls
- Understanding the hardware and software on an enterprise and where it is located and how it should be configured is the foundation of a good security posture
- Not keeping an eye on what is present can be detrimental when working to understanding potential problems
  - Vulnerabilities could fly under the radar and leave an organization vulnerable
- Automated systems can help keep up with asset inventory as well as the patch state of those assets

Authentication Issues

- Authentication is essential in maintaining security
- Authentication issues, e.g. using default usernames and/or passwords, ultimately result in vulnerabilities
- Most systems log sign-in attempts and exits, but the sign-in failures can be very telling of possible malicious behavior

Authentication Issues cont.

- Attackers can even distribute their attacks across multiple usernames to lower the number of failed attempts across accounts

- This type of action could be hard to discover in logs, but SIEM devices could be of use for finding patterns
  - One such pattern would be if the same IP address was used for all attempts

Mobile Devices
Technologies & Tools

Reference:

Drew Hamilton Lecture Notes

DeMarcus Thomas

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

Mobile Devices

- Mobile device use, cloud storage capabilities, and Software as a Service (SaaS) platforms have all converged to produce a very interesting climate
- Mobile devices are everywhere and need to access data constantly
- This has greatly changed how corporate enterprises and personal device usage work together
- The BYOD paradigm is here for the long haul

Connection Methods

- There are a number of different options available for mobile device connectivity
- This section will walk through some of the major options available

Cellular

- Uses mobile telephony circuits and largely use 4G and LTE
- A benefit of this connection type is the widespread availability of signals
- Downside is that services can still have gaps in areas that are remote

Wi-Fi

- Radio communication method developed under the Wi-Fi Alliance
  - System operates on the 2.4- and 5-GHz frequency spectrums
  - Networks are created from your associated enterprise as well as third parties

- Ubiquitous platform that is one of the main methods for building a network today

SATCOM

- Uses terrestrial transmitters and receivers and satellites in orbit for communication
- Normally used in areas in the wilderness and at sea where it is one of the only viable options
- Expensive option compared to other communication technology and can have line-of-sight performance issues

Bluetooth

- Short range low power wireless protocol that transmits in the 2.4 GHz band
  - Primarily designed to transmit data in personal area networks (PANs)
  - Normally has a range of about 32 ft.
- Bluetooth has gone through a number of development iterations and currently is on Bluetooth 4.0
- Security vulnerabilities come into play during protocol advertisement of services and pairing

Near Field Communications (NFC)

- Designed to establish radio communications when devices are within 10 cm of one another or less
- Regained popularity to be used in smartphone and mobile payment systems
- The short distance requirement was designed mainly for security, while apps that use the technology normally have their own security mechanisms as well

ANT

- Multicast wireless sensor network technology
- Similar to Bluetooth 4.0, but is designed to work with heart rate monitors, fitness devices and personal devices
- Uses a unique isosynchronous network technology that allows it to manage communications in a crowded 2.4-GHz spectrum, and to work well with multiple devices without interference.

Infrared (IR)

- Used in remote-control devices for years
- Was first used in networking to connect to printers
- Now used in wireless keyboards and mice
- Slow compared to other technologies and cannot penetrate through walls
- All devices in range can see IR, so security must be on top of the base transmission mechanism

Universal Serial Bus (USB)

- Standard for connecting devices with cables
  - Can be used to transmit data and charge the battery of devices
- One of the most interesting uses with USB is for portable flash memory
- USB flash drives have caused many security problems, with their ability to automount once plugged in
  - Malicious actors can use the characteristics of USB for malicious intent

Universal Serial Bus (USB) cont.

- USB comes in a number of different sizes
  - USB, USB2 USB3
  - USB mini
  - USB micro
  - USB Type-C

Mobile Device Management Concepts

- **MDM policies provide a comprehensive set of security constraints for corporations to follow**
  - **They should require:**
    - **Device locking with a strong password**
    - **Encryption of data on a device**
    - **Device locking automatically after a certain period of inactivity**
    - **The capability to wipe the device automatically after a certain number of failed login attempts**
    - **The capability to remotely wipe the device if it is lost or stolen**

Application Management

- Mobile applications provide many benefits, but also introduce security concerns
- Many apps request a number of different permissions to perform its actions and this can conflict with what organizations are comfortable with allowing
- Organizations have two options, restrict access to prohibited apps through the MDM or, in a more extreme case, develop its own enterprise app store of acceptable applications

Content Management

- Set of actions used to control content issues on mobile devices as far as files that can be accessed and what apps are acceptable

- Organizations normally have policies that state that they have ownership of data even if it resides on the employees personal devices

Remote Wipe

- With mobile devices prevalent, there is an increased need to protect against stolen or lost technology
- If a device is stolen, the thief can use all of his/her resources available to gain access to the data on the phone
- With this concern in mind, this fuels the decision to have remote wiping capability
  - Wiping can be application specific
    - Outlook, calendar, contacts
  - Apple and Android devices have the ability to set up remote locking and factory reset

Geofencing

- Developing a virtual fence for detecting when mobile devices have entered a certain area
- This is done by using GPS and/or radio frequency identification (RFID) technology
- They have been used in marketing to communicate with customers and have been used with workers at remote sites
  - In the latter case when detected, network connections could be enabled for them
  - Geofencing could be even more heavily used in the future

Geolocation

- Heavily relied upon by many apps which use GPS location
  - Device-locating services
  - Mapping applications
  - Traffic monitoring apps
- The location and movement of the device, geolocation, can be used to help apps make recommendations about its surroundings
- It can also be used to help recovery lost devices

Screen Locks

- It is strongly encouraged that security PINs or passcodes are enforced for all mobile devices
- Also the strength of the passcode or PIN should be consistent with your corporate's password policy
- Apple has enabled features such as automatically wiping a device after a specific number of failed login attempts and allows devices to be locked from a user's iCloud account
- Android has a number of features as well
  - Allows some apps to manage the lock screen

Push Notification Services

- Most devices allow for push notifications to update content on a device
- This enables information from external sources to be sent to devices
  - This introduces some security concerns
- It's possible for an external source to have a device emit sound, even if the sound on the device is muted

Passwords and Pins

- Essential measure for keeping mobile devices secure
- Avoid simple solutions for both pins and gesture passcodes
- Be mindful that with gesture based solutions potential thefts could use the oil based patterns on the screen to unlock the phone
- Keep the phone clean or dirtying the whole screen is a method to protection against this

Biometrics

- Are not used on some mobile devices as a means of access control
- These methods have been fallible in the past as shown by many security presentations
  - Screen unlocking via facial recognition is the next step in subverting biometric sensors
- With holes in these security mechanisms, corporate policy should dictate that they not be used to secure sensitive data

Context-Aware Authentication

- This method uses the characteristics of the requests and the connection method to determine if access should be permitted
- Banks and social media apps often do this if your normal routines change or you attempt to login from a different location
- Goal is to protect against unauthorized users, devices, or network connection from accessing corporate data

Containerization

- Provides the ability to separate work-related materials and personal data
- Some MDM systems allow for the encryption of work related containers and allow for the organization to have remote control over that container as well

Storage Segmentation

- Mechanism that allows the separation of where personal data and work data is stored
- Similar idea to containerization in that it provides a logical separation of the storage on a device
- Highly recommended for devices with very sensitive corporate data

Full Device Encryption

- Similar idea to laptops that have full disk encryption
- Mobile devices are more likely to be stolen, so it makes sense to encrypt the organization's mobile devices
- This is emerging technology and vendors should be vetted before making a decision

Enforcement and Monitoring

- The big thing to remember is that security policies for mobile devices should be consistent with other computer security policies
- Disciplinary action should be consistent as well
- You should also have monitoring programs that apply to mobile devices in your organization as well as other systems

Third-Party App Stores

- Two most common app stores
  - The Apple App Store for iOS
  - Google Play for Android devices

- Third-Party apps introduce a number of different security risks because potentially fraudulent apps could reside on the same device as sensitive business data
  - For enterprise devices the app stores could be restricted
  - This becomes more difficult for users accessing business data on their own personal devices

Rooting/Jailbreaking

- Jailbreaking is the process of escalating a user's privilege level to get around restrictions instituted by the OS
  - From a security perspective the thought of raising privileges can cause more problems because normal security mechanisms are bypassed
- Rooting refers to bypassing OS controls and is the term used for Android devices

Rooting/Jailbreaking cont.

- For either case both actions result in OS controls created to restrict operations no longer being effective
  - In most cases this does not increase the security capabilities of a device

Sideloading

- Process of adding apps to a mobile device without using the authorized store associated with the device
- This is possible for Android and Android-like (Kindle Fire) devices
- Without the screening of the authorized app store the odds of loading malicious applications increase

Custom Firmware

- Firmware that has been altered from the original factory settings
- Firmware can bring additional functionality, but also introduces new security concerns
- Should only be used on devices that do not hold critical information

Carrier Unlocking

- Removing the restriction of only being able to use a specific phone carrier
- If a subscriber identity module (SIM) card from a different carrier is inserted, the phone will not work
- Normally there is a special input sequence on the phone that allows for the device to be unlocked and freed to be used with different carriers

Firmware OTA (over the air) Updates

- Just like any other software, eventually firmware will require updates
- With the scale of mobile devices it is not feasible to have a central location where all users can bring their phone to be updated
- OTA updates solve this problem
  - Similar to you updating apps via the app store, you can also update device firmware from device manufacturers

Camera Use

- Most mobile devices have an on-board camera that could be used to disseminate sensitive information
- They could also be used to perform illegal activity
  - If done with a company-owned phone this causes liability issues for the company
- A concern for the users/employees is that their personal pictures could be deleted by a wipe command that originated from the organization

SMS/MMS

- Both of these are standard messaging protocols used to send normal and picture messages on your phone

- Because potential sensitive information can be sent over these two methods, you must also address this form of communication in any associated policies

External Media

- Refers to any type of device that is capable of storing data
  - Music players
  - Phones
  - Tables
  - Smart Watches
  - USB devices
  - Etc.
- All of these items are potential avenues for data exfiltration
- An effective policy is very clear as to where these types of devices will be permitted and where they will be banned

USB OTG

- Universal Serial Bus is the standard for connecting mobile devices to computers

- USB OTG (on-the-go) allows for devices that support this to be connected directly to one another
  - The device can switch back and forth between roles
    - Who provides power verse consumes
    - Who sends data vs receives
  - Most devices made after 2015 are USB OTG compatible

Recording Microphone

- Many mobile devices enable some type of recording functionality
- This introduces another security concern when it comes to collecting sensitive data without the parties under observation being aware
- Rules must be established for when such recording is permissible

GPS Tagging

- **Photos taken on mobile devices or with cameras that have GPS enabled can have location information embedded in the digital photos**
  - **CompTIA calls this GPS tagging while others call it Geo-tagging**

- **Having this service enabled can inadvertently advertise personal information**
  - **Potential information disclosure:**
    - **Home address**
    - **Place of employment**
    - **Location of love ones**
    - **Etc.**

Wi-Fi Direct/Ad Hoc

- **Wi-Fi Direct permits one devices to connect directly to one other device**
  - **Connection can be established with WPA2**
  - **Use Wi-Fi Direct Device and Service Discovery**
    - **Filters the devices that can be connected based on the services both devices support**
      - **Device could filter based on what other devices allow printing services**

- **Wi-Fi ad hoc networks allow multiple devices to communicate with each other, with each device capable of communicating with all other devices**

Tethering

- Connection of a device to a mobile device that is sharing its network access

- Descriptions:
  - Tethering is not connecting a phone to a laptop to charge
  - Tethering is connecting your laptop to your phone to get on the Internet

Payment Methods

- Payment methods have become more diverse with the introduction of using smart devices and Near Field Communication (NFC) that can link to credit or debit cards

- The digital devices actually provide some additional security features, NFC, biometrics/pin, that normally would not be available with traditional payment methods

Deployment Models

- When considering a deployment model, there are a number of different parameters that must be taken into consideration
  - How will security be enforced?
  - What devices will be supported?
  - How will policies be enforced?
- Based on how those questions are answered, you can choose your deployment model
- It must be understood that there are still advantages and disadvantages to each model

BYOD

- Bring Your Own Device
- Allows companies to reduce cost of providing devices to all employees
- Employees tend to want a single device for all of their needs
- Good for small firms or organizations with a number of temporary workers
- The organization has limited control over the user owned personal device

CYOD

- Choose your own device
- Allows users to select the device they would like from a limited selection
- Organization has more flexibility in what they control since they own the device
  - App selection
  - Data restrictions
  - Updates
  - Etc.

COPE

- Corporate, owned, personally enabled
- Organization chooses a phone for the employee, but allows them to use it for personal activities
- Organization can set boundaries on what types of personal activities can be performed on the device
- Organization is still in control of the security functionality while employee receives “some” freedom of use

Corporate-Owned

- Corporate-owned, business only
- Employees receive phone that is to be used for business use only
- Disadvantage is the need for employees to have two phones
- Advantage is that the company has complete control over all aspects of the device

Virtual Desk Interface (VDI)

- Deployment models are not just limited to mobile devices
- Personal computers can also be external mobile devices requiring remote connections
- One solution to this problem for laptops is to implement a virtual desktop infrastructure solution
  - Helps to bring control to the mobile environment associated with non-corporate-owned equipment

VDI cont.

- Fully security compliant virtual desktop machines are setup with all the applications needed for the employee and they can simply connect to this machine via virtual connection or remote desktop

- Does require an effective IT staff that can manage this technology for the organization

Implementing Secure Protocols Technologies & Tools

Reference:

Drew Hamilton Lecture Notes

DeMarcus Thomas

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

Implementing Secure Protocols

- Protocols act as a language that give the ability for different components to be able to communicate from a set of known commands
- There are protocols that exist that have built-in security mechanisms that secure communication without any additional effort
- This section will discuss security enabled protocols

DNSSEC

- Domain Name Service (DNS) translates names into IP addresses
- Can also be used for e-mail delivery
- Uses UDP over port 53 in most instances to perform inquiries
  - For larger zone transfers TCP can be used
- DNS is one of the primary protocols used on the Internet and is involved in almost all addressing lookups

DNSSEC cont.

- Issue with DNS is requests are sent in plain-text and are subject to spoofing
- DNSSEC is a set of extensions to DNS that use cryptography to support
  - Orgin authentication
  - Authenticated denial of existence
  - Data integrity
- All DNS records can now be signed, but not encrypted

SSH

- Protocol used to establish encrypted remote terminal connections to servers
- Uses asymmetric encryption, but generally requires an independent source of trust with a server
  - Manually receives a server key to operate
- Uses TCP port 22 as its default port
- Designed as a secure alternative to Telnet

S/MIME

- Multipurpose Internet Mail Extensions (MIME) is the standard for transmitting binary data via an e-mail
- MIME specifies how plain-text as well as any attachment should be encoded to successful transmit
- There is no security associated with this protocol and anyone between the sender and receiver can see all information transmitted

S/MIME cont.

- S/MIME is the standard for public key encryption and signing of MIME data in emails
- Built into most modern e-mail software so that it can interoperate smoothly and provides cryptographic protection to email

SRTP

- Secure Real-time Transport Protocol
- Network protocol designed to securely deliver audio and video over IP networks
- Uses cryptography to provide encryption, message authentication and integrity, and replay protection to the RTP data

LDAPS

- Lightweight Directory Access Protocol is used to provide organized sets of records as a hierarchical structure
  - Used in Active Directory datasets
- By default LDAP communications are insecure
- LDAP is secured using SSL/TLS using a certificate from a trusted certificate authority (CA)

FTPS

- This is the secure versions of the File Transfer Protocol over an SSL/TLS channel
- Fully FTP compatible
- Uses TCP ports 989 and 990

SFTP

- FTP protocol over an SSH channel
- Uses the encryption protections of SSH to secure FTP transfers
- Uses TCP on port 22

SNMPv3

- Simple Network Management Protocol version 3
- It is an application layer protocol and the standard for managing devices on IP-based networks
- Uses port 161 and 162 and both must be open on a firewall

SSL/TLS

- Secure Sockets Layer / Transport Layer Security
- SSL is an application of encryption technology developed for transport-layer protocols
- Uses public key encryption to exchange a symmetric key
  - Use to provide confidentiality and integrity protection and as well as authentication
  - It has been replaced by TLS
- TLS uses the same principles of SSL, but with updated mechanisms

HTTPS

- Hypertext Transfer Protocol Secure is the use of SSL or TLS to encrypt a channel over which HTTP traffic is transmitted
- Because of security concerns with SSL, only TLS is recommended to be used
- HTTP uses port 80, but with HTTPS it uses TCP 443

Secure POP/IMAP

- Refered to as POP3 and IMAP on CompTIA exam
- Encrypts data from an e-mail client sent to the e-mail server or SSL/TLS session
- If unsecure modes are initiated for an e-mail connection the STARTTLS directive tells the client to change to secure ports
  - POP3 uses port 110, Secure POP3 uses TCP port 995
  - IMAP uses port 143, Secure IMAP uses TCP port 993

Use Cases

- Protocols enable parties to have an upfront understanding as to how communication will be managed
- Parties will communication in different ways for different reasons
  - As a result, there are different use cases for different protocols
- This section will highlight some of the common use cases for the protocol discussed previously

Voice and Video

- Voice and video are frequently streaming media and have protocols dedicated to encoding data streams

- To securely transmit media SRTP can be used
  - Securely delivers audio and video over IP networks

Time Synchronization

- Network Time Protocol is the standard for time synchronization across servers and clients
- It has no inherent security built in and is transmitted over UDP port 123
  - It is susceptible to main-in-the-middle attacks
- Can be secured by enclosing communications using a TLS tunnel

Email and Web

- **Both native plaintext-based systems**
- **Email uses S/MIME and Web uses SSL/TLS (With TLS being the preferred option)**

File Transfer

- Secure file transfer can be accomplished via a wide range of methods, ensuring the confidentiality and integrity of file transfers across networks

- SFTP and FTPS are both secure alternatives to the insecure FTP

Directory Services

- Directory services use LDAP as the primary protocol
- LDAPS is the common option when security is required
  - Commonly found behind the scenes for logon information

Remote Access

- **Remote Access**
  - **Accessing computer resources across a network**
  - **This can be done in many ways**
    - **For securing actual channels of information and data in transit SSL/TLS is used**
    - **When accessing devices such as routers and switches, SSH is used**
    - **For servers and other computer connections, VPN or IPSec is common**

Domain Name Resolution

- **DNSSEC is the secure alternative to DNS but has not been widely deployed yet**

- **The protocol has been available for local deployments since able 2012**

Routing and Switching

- These are the backbone functions of networking in a system and are managed by using SNMPv3
  - Enables applications to manage data associated with networking and devices

- Local access to boxes should be accomplished with SSH

Network Address Allocation

- SNMPv3 can help manage information to perform network assignments
- IP addresses can either be assigned statically or via the DHCP protocol or a combination of both

Subscription Services

- Is the problem of managing data flows to and from a system based on either a push (publish) or pull (subscribe) model
- This can be managed by using LDAP
  - Protocol has to understand which data elements are needed by which nodes

Summary

- Network Components
- Security Tools and Technologies
- Troubleshooting Common Security Issues
- Mobile Devices
- Implementing Secure Protocols