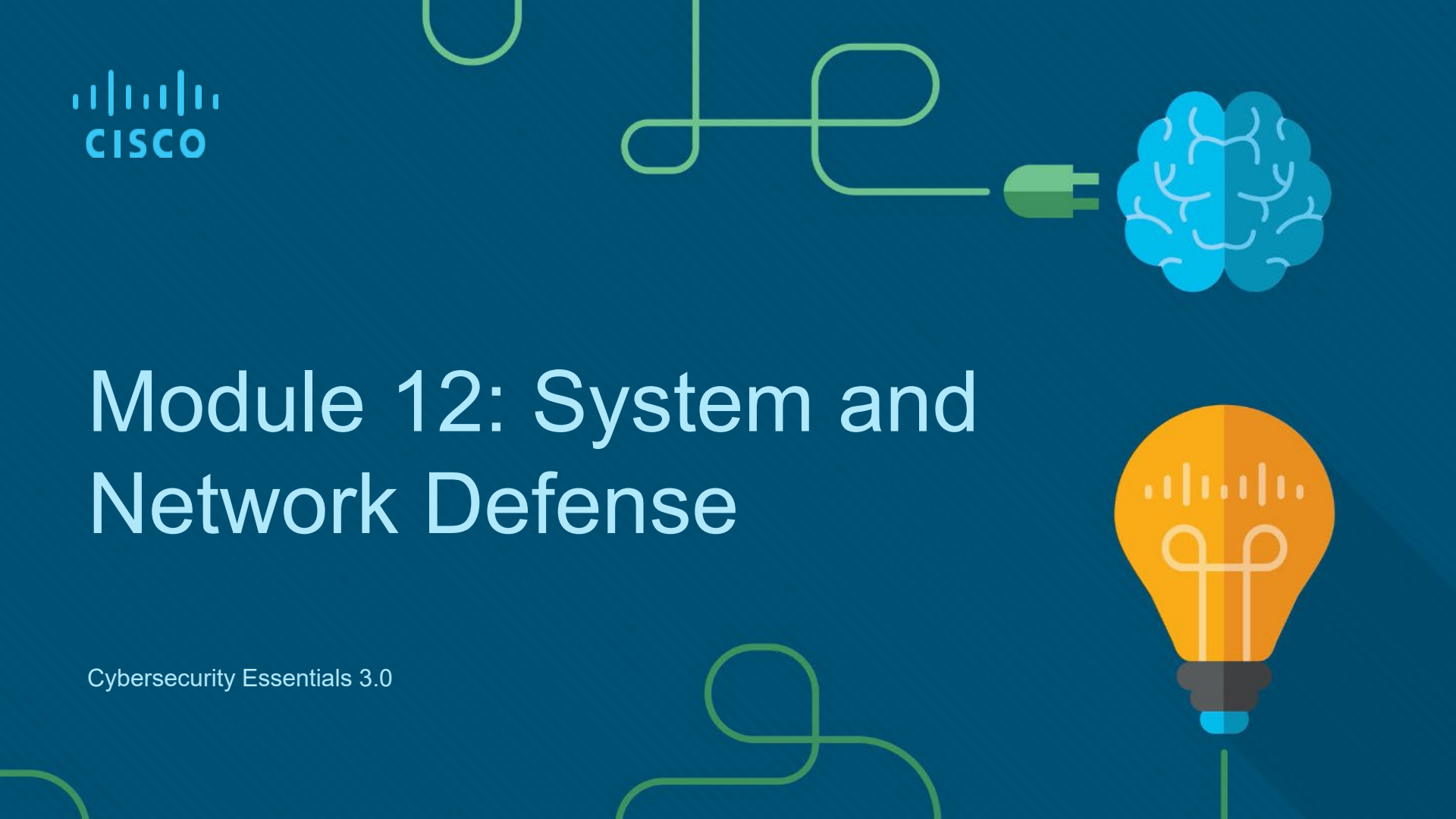


Module 12: System and Network Defense

Cybersecurity Essentials 3.0

Module Objectives

Module Title: System and Network Defense

Module Objective: Implement some of the various aspects of system and network defense.

Topic Title	Topic Objective
Physical Security	Explain how physical security measures are implemented to protect network equipment.
Application Security	Explain how to apply application security measures.
Network Hardening: Services and Protocols	Explain how to harden network services and protocols.
Network Hardening: Segmentation	Explain how network segmentation can help you harden the network.
Hardening Wireless and Mobile Devices	Configure wireless router hardening and security.
Cybersecurity Resilience	Explain physical security with IoT devices.
Embedded and Specialized Systems	Implement physical security with IoT devices.

12.1 Physical Security

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Fencing and Physical Barriers

- Barricades or fencing are often the first things that come to mind when thinking about types of physical security.

- In many situations, they are the outermost layer of defense and the most visible. All physical barriers should meet specific design requirements and material specifications.

Physical barriers may have the following components:

- Perimeter fence system
- Security gate system
- Bollards (short posts used to stop vehicle intrusions)
- Vehicle entry barriers
- Guard shelters
- Fencing

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Fencing and Physical Barriers (Cont.)

A **fence** is a barrier that encloses secure areas and designates boundaries.

When designing a perimeter fencing system, the following height guidelines apply:

- 1 meter (3-4 ft.) will only deter casual trespassers.
- 2 meters (6-7 ft.) are too high to climb by casual trespassers.
- 2.5 meters (8 ft.) will offer limited delay to a determined intruder.

- High-security areas often require a ‘top guard’ such as barbed wire or concertina wire.
- Local regulations may restrict the type of fencing system an organization can use and it’s important to remember that fences require regular maintenance.
- Moreover, vehicles should never be parked near a security fence, as this could assist the intruder in climbing over or causing damage to the fence.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Biometrics

- Biometrics are the physiological or behavioral characteristics of an individual, and there are security practices based on identifying and granting access using biometrics.
- Biometric authentication systems can include measurements of the face, fingerprint, hand geometry, iris, retina, signature and voice.
- Biometric technologies can be the foundation of highly secure identification and personal verification solutions.
- Biometrics can ensure confidential financial transactions and personal data privacy — a well-known example being smartphones which use fingerprint readers to unlock the device and access apps, including online banking and payment systems.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Biometrics (Cont.)

When selecting biometric systems, there are several important factors to consider, including:

- Accuracy
- Speed or throughput rate
- Acceptability to users
- Uniqueness of the biometric organ and action
- Resistance to counterfeiting
- Reliability
- Data storage requirements
- Enrollment time
- Intrusiveness of the scan

The most important of these factors is accuracy, which is expressed in error types and rates.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Biometrics (Cont.)

- In many biometric applications, particularly retail or banking, false rejections (Type I error) can have a very negative impact on business due to a transaction or sale being lost.

- False acceptance is a Type II error. Type II errors allow entry to people who should not have entry, meaning a cybercriminal can potentially gain access.
  - For this reason, Type II errors are normally considered the most important error for a biometric access control system.

- The acceptance rate is also an important concept here. Stated as a percentage, it is the rate at which a system accepts unenrolled individuals or imposters as authentic users – so the rate of Type II errors per total instances of granting permission.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Surveillance

Many physical access controls, including deterrent and detection systems, ultimately rely on people to intervene and stop the actual attack or intrusion.

- **Video and Electronic Surveillance** can supplement or, in some cases, replace security guards.
- The benefits of video and electronic surveillance include the ability to monitor areas when no other persons are present, the ability to record and log surveillance videos and data for long periods, plus being able to link to motion detection technology and notifications where appropriate.
- In a highly secure environment, video and electronic surveillance should be placed at all entrances, exits, loading bays, stairwells, and refuse collection areas.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Surveillance (Cont.)

- **Guards and Escorts:** Security guards are a great solution for access control requiring an instantaneous and appropriate response.
- Disadvantages include cost and the inability to monitor and record high volumes of traffic, and the risk of human error.
- In highly secure information system facilities, guards control access to the organization's sensitive areas.
- The benefit of using guards here is that they can adapt more than automated systems. Guards can learn and distinguish many different conditions and situations and make decisions on the spot.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Surveillance (Cont.)

- **RFID and Wireless Surveillance:** Managing and locating important information system assets is a key challenge for most organizations.
  - Growth in the number of mobile and IoT devices has made this job even more difficult.
  - The use of Radio Frequency Identification (RFID) asset tags can be of great value to the security staff.
    - An organization can place RFID readers in the door frames of secure areas so that they are not visible to individuals.
    - The benefit of RFID asset tags is that they can track any asset that physically leaves a secure area.
    - New RFID asset tag systems can read multiple tags simultaneously.
    - RFID systems do not require line-of-sight to scan tags, either.
    - Another advantage of RFID is the ability to read tags that are not visible.
    - Unlike barcodes and human-readable tags that must be physically located and openly displayed to read, RFID tags do not need to be visible to scan.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

12.2 Application Security

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Application Development

To maintain security at all stages of application development, a robust process needs to be followed.

- **Developing and testing:** Software is developed and updated in a development environment, where it can be developed, tested and debugged before being deployed.
  - A development environment is less restrictive than the live environment and has a lower security level.
  - Version control software helps track and manage changes to the software code.
  - Developers may also work in a sandbox environment so that code is not overwritten as they develop it.

- During testing, developers look at how the code interacts with the normal environment.
  - Quality assurance (QA) can find defects in the software.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Application Development (Cont.)

- **Staging and production:** Staging environments should closely match the organization's production environment.
  - By testing in a staging environment, developers can verify that the software runs under the required security settings.
  - After the developer runs and tests security, the program can be deployed to production.

- **Provisioning and deprovisioning:** Provisioning is the creation or updating of software. Deprovisioning is its removal.
  - An organization can use a self-service portal to automate software provisioning and deprovisioning.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Security Coding Techniques

When coding applications, developers use several techniques to validate that all security requirements have been met.

- **Normalization** is used to organize data in a database and help maintain data integrity. Normalization converts an input string to its simplest known form to ensure that all strings have unique binary representations and that any malicious input is identified.

- A **stored procedure** is a group of precompiled SQL statements stored in a database that execute a task. If you use a stored procedure to accept input parameters from clients using different input data, you will reduce network traffic and get faster results.

- **Obfuscation** hides original data with random characters or data. **Camouflage** replaces sensitive data with realistic fictional data. A developer can use obfuscation and camouflage to prevent software from being reverse engineered.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Security Coding Techniques (Cont.)

- **Code reuse** means using existing software to build new software, saving time and development costs. Care must be taken, though, to avoid the introduction of vulnerabilities.

- **Software development kits (SDKs)** and third-party libraries provide a repository of useful code to make application development faster and cheaper.
  - The downside is that any vulnerabilities in SDKs or third-party libraries can potentially affect many applications.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Input Validation

- Controlling the data input process is key to maintaining database integrity.
  - Many attacks run against a database and insert malformed data.
  - Such attacks can confuse, crash or make the application divulge too much information to the attacker.

- Customers fill out a web application form to subscribe to a newsletter.
  - A database application automatically generates and sends email confirmations back to the customers.
  - When customers receive the email with a URL link to confirm their subscription, attackers have modified the URL link.
  - These modifications can change the username, email address or subscription status of the customers when they click to confirm their subscription.
  - Hackers can automate this attack to flood the web application with thousands of invalid subscribers to the newsletter database.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Validation Rules

A validation rule checks that data falls within the parameters defined by the database designer. A validation rule helps to ensure the completeness, accuracy, and consistency of data. The criteria used in a validation rule include the following:

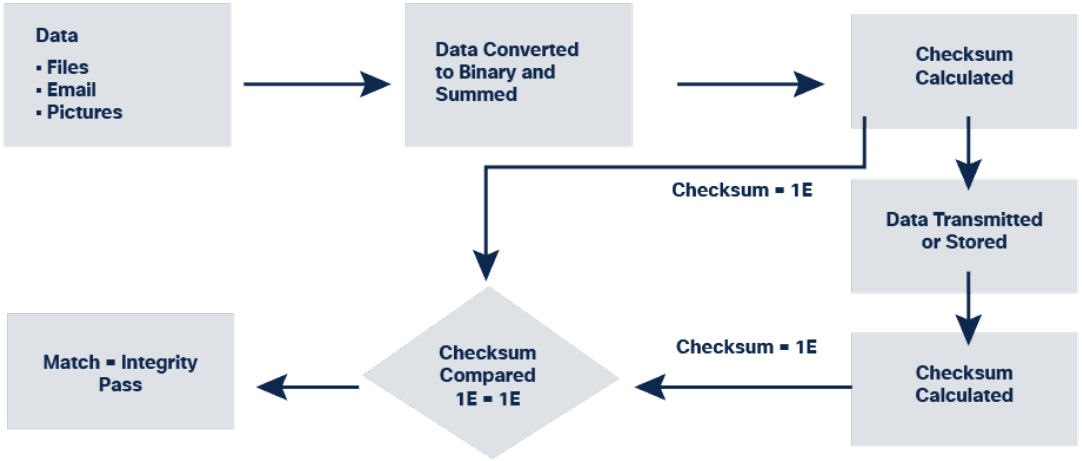
- **Size** – checks the number of characters in a data item
- **Format** – checks that the data conforms to a specified format
- **Consistency** – checks for the consistency of codes in related data items
- **Range** – checks that data lies within a minimum and maximum value
- **Check digit** – provides for an extra calculation to generate a check digit for error detection

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Integrity Checks

Compromised data can threaten the security of your devices and systems.

An **integrity check** can measure the consistency of data in a file, picture or record to ensure that it has not been corrupted. The integrity check performs a **hash function** to take a snapshot of data and then uses this snapshot to ensure data has remained unchanged. A **checksum** is an example of a hash function.



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Integrity Checks (Cont.)

How a checksum works:

- A checksum verifies the integrity of files, or strings of characters, before and after they transfer between devices across a local network or the Internet.
  - Checksums convert each piece of information to a value and sums the total.
  - To test the data integrity, a receiving system repeats the process. If the two sums are equal, the data is valid. If not, a change has occurred somewhere along the line.

Hash functions:

- Common hash functions include MD5, SHA-1, SHA-256 and SHA-512.
  - These use complex mathematical algorithms to compare data to a hashed value.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Integrity Checks (Cont.)

Version control:

- Organizations use version control to prevent authorized users from making accidental changes.
  - Version control means that two users cannot update the same object, such as a file, database record or transaction, at the exact same time.

Backups:

- Accurate backups help to maintain data integrity if data becomes corrupted.
- An organization needs to verify its backup process to ensure the integrity of the backup.

Authorization:

- Authorization determines who has access to an organization's resources based on a need-to-know basis.
  - For example, file permissions and user access controls ensure that only certain users can modify data.
  - An administrator can set permissions for a file to read-only.
    - As a result, a user accessing that file cannot make any changes.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Other Application Security Practices

How can you be sure that a piece of software you are installing is authentic or that information is secure when browsing the Internet?

Code signing helps prove that a piece of software is authentic.

- Executables designed to install and run on a device are digitally signed to validate the author's identity and provide assurance that the software code has not changed since it was signed.

Secure cookies

- Using secure cookies protects information stored in cookies from hackers.
- When your client system interacts with a server, the server sends an HTTP response that instructs your browser to create at least one cookie.
  - The cookie then stores data for future requests while you are browsing that website.

- Web developers should use cookies with HTTPS, to secure cookies and prevent them from being transmitted over unencrypted HTTP.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Managing Threats to Applications

Organizations can implement various measures to manage threats to the application domain.

Unauthorized access to data centers, computer rooms, and wiring closets:

- Implement policies, standards, and procedures for staff and visitors to ensure the facilities are secure.

Server and system downtime:

- Develop a business continuity plan for critical applications to maintain availability of operations.
- Develop a disaster recovery plan for critical applications and data.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Managing Threats to Applications (Cont.)

Network operating system software vulnerability:

- Develop a policy to address application software and operating system updates.
- Install patches and updates regularly.

Unauthorized access to systems:

- Use multi-factor authentication.
- Monitor log files.

Data loss:

- Implement data classification standards.
- Implement backup procedures.

Software Development Vulnerabilities:

- Conduct software testing prior to launch.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab - Investigating OWASP

In this lab, you will complete the following objectives:

- Part 1: OWASP Top 10
- Part 2: OWASP Community Pages

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

12.3 Network Hardening: Services and Protocols

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network and Routing Services

- Cybercriminals use vulnerable network services to attack a device or to use it as part of an attack.
- To check for insecure network services, use a port scanner to detect open ports on a device.
- A port scanner sends a message to each port and waits for a response, which indicates how the port is used and whether it is open.
  - Cybercriminals also use port scanners for this same reason.
  - Securing network services ensures that only necessary ports are exposed and available.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network and Routing Services (Cont.)

Dynamic host configuration protocol (DHCP) uses a server to assign an IP address and other configuration information to network devices.

- In effect, the device gets a permission slip from the DHCP server to use the network.
- Attackers can target DHCP servers to deny access to devices on the network, but security measures like DHCP snooping prevent rogue DHCP servers from providing IP addresses to clients by validating messages from sources that are not trusted.

- A security checklist for DHCP:
  - Physically secure the DHCP server.
  - Apply any software patches.
  - Locate the DHCP server behind a firewall.
  - Monitor DHCP activity by reviewing DHCP logs.
  - Maintain a strong antivirus solution.
  - Uninstall any unused services and applications.
  - Close unused ports.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network and Routing Services (Cont.)

Domain name system (DNS) translates a URL or website address, such as www.cisco.com, into a numerical IP address. When users type a web address into the address bar, the DNS server will recognize the IP address.

DNS Security Extensions (DNSSEC) uses digital signatures to strengthen authentication and protect against threats to the DNS.

- A security checklist for DNS:
  - Keep DNS software up to date.
  - Prevent version string from revealing information.
  - Separate internal and external DNS servers.
  - Restrict allowed transactions by client IP address.
  - Use transaction signatures to authenticate transactions.
  - Disable or restrict zone transfers and dynamic updates as much as possible.
  - Enable logging and analyze logs.
  - Use Domain Name System Security Extensions (DNSSEC).
  - Sign zones.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network and Routing Services (Cont.)

Internet control messaging protocol (ICMP): Network devices use ICMP to send error messages that a requested service is not available, or the host could not reach the router, for example.

- The ping command is a network utility that uses ICMP to test the reachability of a host on a network.
  - Ping sends ICMP messages to the host and waits for a reply.
  - Cybercriminals can alter the use of ICMP to run reconnaissance, denial of service (DoS) and covert channel attacks.
  - Many networks filter ICMP requests to prevent such attacks.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network and Routing Services (Cont.)

Routing information protocol: RIP is a routing protocol that limits the number of hops from source to destination that are allowed in a network path.

- The maximum number of hops allowed for RIP is fifteen.
- RIP is used to exchange routing information about which networks each router can reach and how far away those networks are.

- RIP calculates the best route based on hop count, but cybercriminals can also target routers and the RIP protocol.
  - Such attacks on routing services can affect performance and availability, some attacks can even result in traffic redirection.
  - Use secure services with authentication and implement system patching and updates to protect routing services.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network and Routing Services (Cont.)

Network Time Protocol (NTP) is a protocol that synchronizes network computer system clocks.

- Having the correct time within networks is important.
  - Correct timestamps accurately track network events such as security violations.
  - Additionally, clock synchronization is critical for the correct interpretation of events within syslog data files as well as for digital certificates.

- NTP allows network devices to synchronize their time settings with an NTP server.
  - Cybercriminals attack timeservers to disrupt secure communication that depends on digital certificates and to hide attack information.
  - Use NTP Authentication to verify that the server is trusted.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Telnet, SSH, and SCP

Secure Shell (SSH) is a protocol that provides a secure (encrypted) remote connection to a device.

Telnet is an older protocol that uses unsecure plaintext when authenticating a device (username and password) and transmitting data.

- SSH should be used rather than Telnet to manage connections, as it provides strong encryption.
  - SSH uses TCP port 22.
  - Telnet uses TCP port 23.

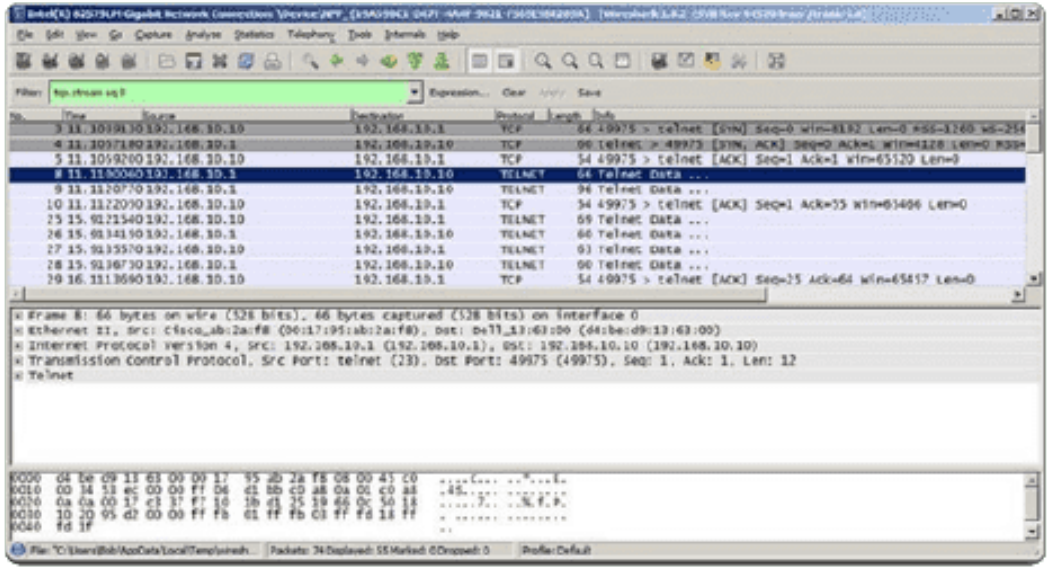
Secure copy (SCP) securely transfers files between two remote systems.

- SCP uses SSH for data transfer and authentication, ensuring the authenticity and confidentiality of the data in transit.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

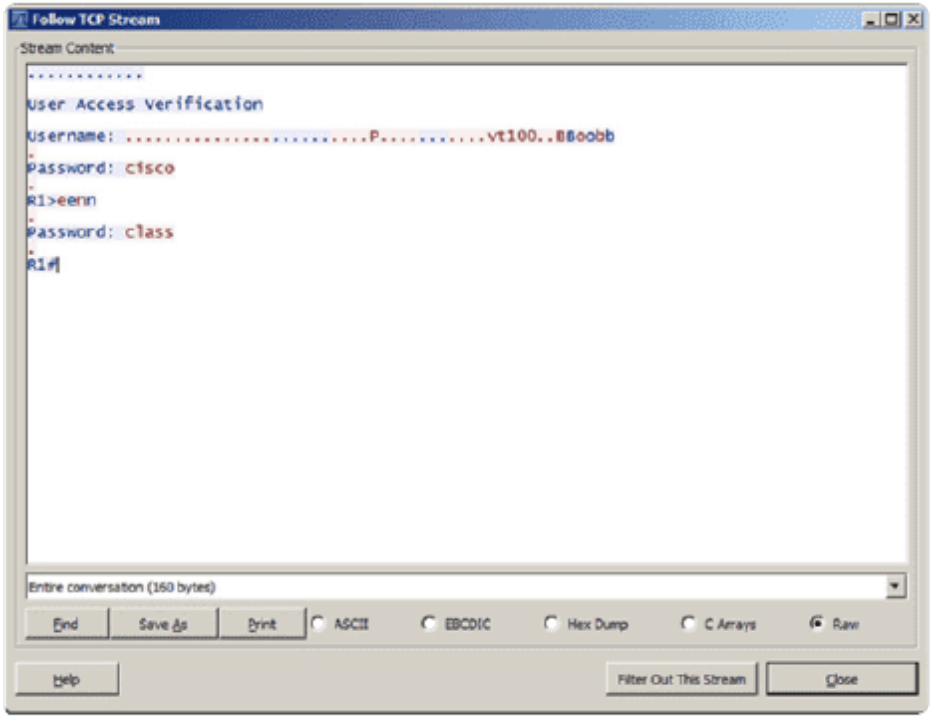
Telnet, SSH and SCP (Cont.)

Wireshark Telnet capture: Cybercriminals monitor packets using Wireshark.



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Telnet, SSH and SCP (Cont.)

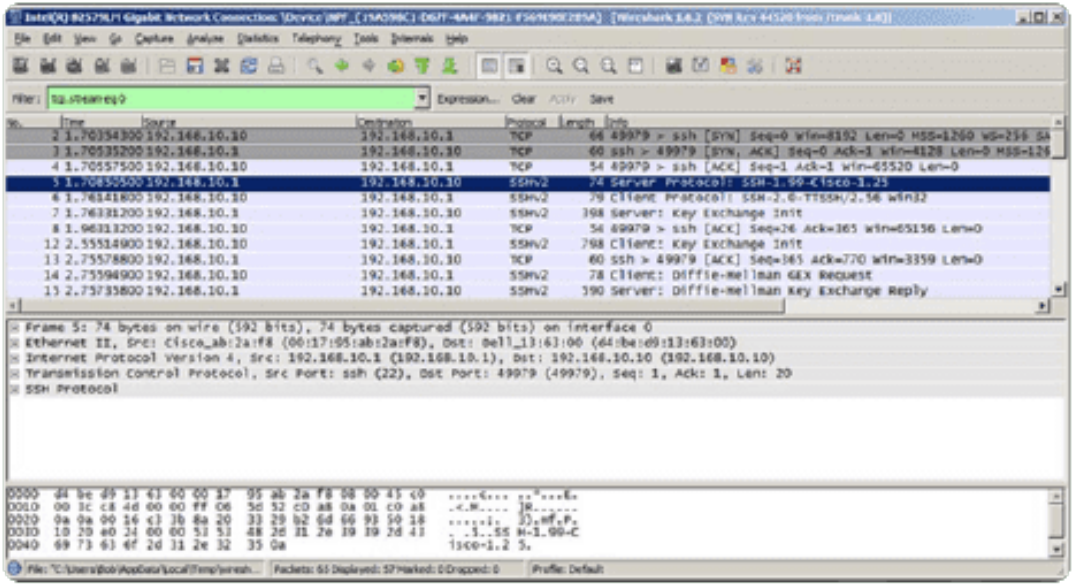


Plaintext username and password capture: Cybercriminals capture the username and password of the administrator from the plaintext Telnet session.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Telnet, SSH and SCP (Cont.)

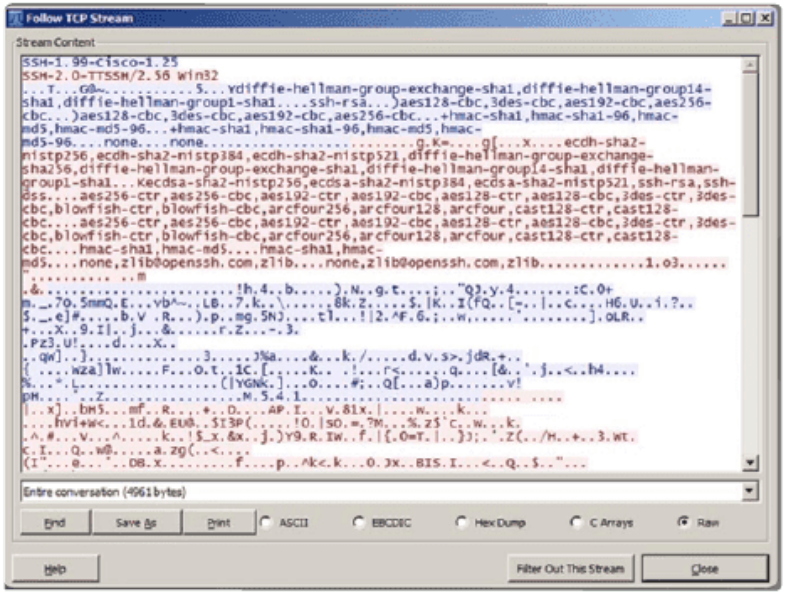
Wireshark SSH capture: The Wireshark view of an SSH session. Cybercriminals track the session using the IP address of the administrator device.



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Telnet, SSH and SCP (Cont.)

Username and password encryption: The session encrypts the username and password.



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Secure Protocols

Attackers can penetrate a network's infrastructure through services, protocols, and open ports.

Simple Network Management Protocol (SNMP) collects statistics from TCP/IP devices to monitor network and computer equipment. SNMPv3 is the current standard — it uses cryptography to prevent eavesdropping and make sure data hasn't been tampered with while in transit.

Hypertext Transfer Protocol (HTTP) provides basic web connectivity and uses port 80. HTTP contains limited built-in security and is open to traffic monitoring when transmitting content, leaving the user's computer open to attack.

- Protocols that provide a more secure connection:
  - **Secure Sockets Layer (SSL)** manages encryption by using an SSL handshake at the beginning of a session to provide confidentiality and prevent eavesdropping and tampering.
  - **Transport Layer Security (TLS)** is an updated, more secure replacement for SSL.
  - SSL/TLS encrypts communication between the client and the server. Where it's used, the user will see HTTPS in the URL field of a browser instead of HTTP.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Secure Protocols (Cont.)

File Transfer Protocol (FTP) transfers computer files between a client and a server. In FTP, the client uses a plaintext username and password to connect. File Transfer Protocol Secure (FTPS) is more secure — it adds support for TLS and SSL to prevent eavesdropping, tampering and forgery on exchanged messages.

Email uses **Post Office Protocol (POP)**, **Internet Message Access Protocol (IMAP)** and **Multipurpose Internet Mail Extensions (MIME)** to attach non-text data, such as an image or video, to an email message.

- To secure POP (port 110) or IMAP (port 143), use SSL/TLS to encrypt mail during transmission.
- The Secure/Multipurpose Internet Mail Extensions (S/MIME) protocol provides a secure method of transmission.
    - It sends digitally signed and encrypted messages that provide authentication, message integrity, and nonrepudiation.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

12.4 Network Hardening: Segmentation

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Virtual Local Area Networks (VLANs)

A **virtual local area network (VLAN)** can be used to segment the network and create a secure area for the sensitive data.

Devices are grouped.

- VLANs provide a way to group devices within a local area network (LAN) and on individual switches.
- VLANs are not the same as LANs: virtual LANs are based on logical connections, while LANs are based on physical connections.
- Individual ports on a switch can be assigned to a specific VLAN.
- Other ports (trunks) can be used to physically interconnect switches and allow multiple VLAN traffic between switches.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Virtual Local Area Networks (VLANs) (Cont.)

The network is segmented.

- VLANs allow an administrator to segment a network based on factors such as function, project, team, or application.
- Devices within a VLAN act as if they are in their own independent network, even though they share a common infrastructure with other VLANs on the same LAN.
- A VLAN can separate groups of devices that host sensitive data from the rest of the network, decreasing the chances of confidential information breaches — in our example, the HR department looking to protect sensitive data.
- Trunks allow individuals on the HR VLAN to be physically connected to multiple switches.

Data is protected.

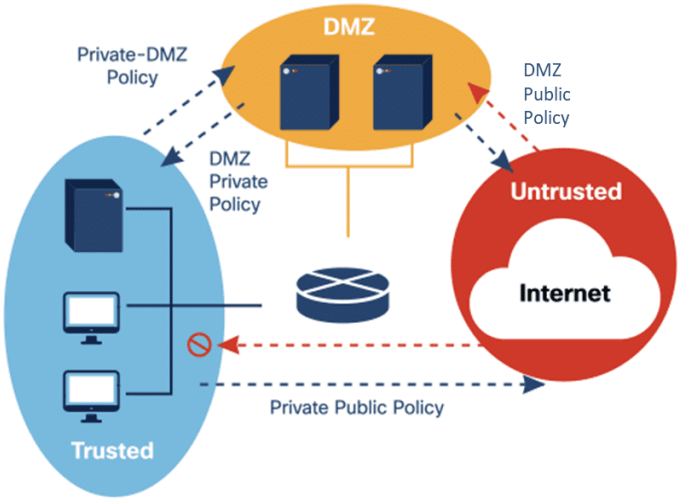
- VLANs provide a way to limit broadcast traffic in a switched network.
- To protect the VLAN, monitor its performance, use advanced configurations, and regularly install patches and updates.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Demilitarized Zone (DMZ)

A demilitarized zone (DMZ) is a small network between a trusted private network and the Internet.

Access to untrusted networks: Web servers and mail servers are usually placed within the DMZ to allow users to access an untrusted network, such as the Internet, without compromising the internal network.



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Demilitarized Zone (DMZ) (Cont.)

Zones of risk: Most networks have two to four zones of risk (the trusted private LAN, the DMZ, the Internet, and an extranet).

- Within the LAN zone, the risk level is low, and the trust level is high.
- Within the extranet zone, the risk level is medium-low, and the trust level medium-high.
- Within the DMZ, the risk level is medium-high, and the trust level is medium-low.
- Within the Internet zone, the risk level is high, and the trust level is low.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Demilitarized Zone (DMZ) (Cont.)

Zero trust model: Firewalls manage east-west traffic (traffic that goes between servers within the organization's data center) and north-south traffic (data moving into and out of the organization's network).

- To protect its network, an organization can implement a Zero Trust model.
- Automatically trusting users and endpoints within the organization can put any network at risk, as trusted users can move throughout the network to access data.
- Zero Trust networking constantly monitors all users on the network regardless of their status or role.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

12.5 Hardening Wireless and Mobile Devices

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Wireless Device Security

Wired Equivalent Privacy (WEP) was the first security protocol used for wireless networks. This was replaced by Wi-Fi Protected Access (WPA), which improved the security of wireless connections.

- **WPA Configuration:** Wi-Fi Protected Access (WPA) was the computer industry's response to the weaknesses of the WEP standard. WPA-PSK (Pre-Shared Key) is the most common WPA configuration. The keys used by WPA are 256-bit, a significant increase over the 64-bit and 128-bit keys used in the WEP system.

- **WPA features:** WPA provided message integrity checks (MIC), which could detect if an attacker had captured and altered data passed between the wireless access point and a wireless client. The Temporal Key Integrity Protocol (TKIP) standard helped to better handle, protect and change encryption keys. Advanced Encryption Standard (AES) superseded TKIP, for even better key management and encryption protection.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Wireless Device Security (Cont.)

- **The Wi-Fi Protected Access II (WPA2)** standard was released in 2006. This introduced the mandatory use of AES algorithms and replaced TKIP with the Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP).

- **The Wi-Fi Protected Access III (WPA3)** WPA3 added more features to WPA2 such as maintaining strong cryptographic algorithms and improving key exchange.

- **Wi-Fi Protected Setup (WPS)** can be used to set up a secure wireless home network. A PIN code is used to connect devices to the wireless network. However, WPS poses a major security vulnerability, as the user's PIN can be discovered through brute-force attack. Due to this, WPS should not be used and should be disabled altogether.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

PT Video - Configure Wireless Router Hardening and Security

This video demonstrates configuring wireless security on a wireless router.

- Part 1: Configure Basic Security Settings for a Wireless Router
- Part 2: Configure Wireless Router Network Security
- Part 3: Configure Wireless Clients Network Security
- Part 4: Verify Connectivity and Security Settings

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Packet Tracer - Configure Wireless Router Hardening and Security

In this Packet Tracer activity, you will complete the following objectives:

Part 1: Configure Basic Security Settings for a Wireless Router
Part 2: Configure Wireless Router Network Security
Part 3: Configure Wireless Clients Network Security
Part 4: Verify Connectivity and Security Settings

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Authentication

Wireless devices have become predominant on most modern networks. They provide mobility and convenience but are vulnerable to a range of cybersecurity issues. They are open to theft, hacking and unauthorized remote access, sniffing, man-in-the-middle attacks, as well as attacks against performance and availability.

- The best way to secure a wireless network is to use authentication and encryption. The original wireless standard, 801.11, introduced two types of authentication.

- **Open system authentication:** Any wireless device can connect to the wireless network. Use this method in situations where security is of no concern.

- **Shared key authentication:** Provides mechanisms to authenticate and encrypt data between a wireless client and AP or wireless router.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Authentication Protocols

The **Extensible Authentication Protocol (EAP)** is an authentication framework used in wireless networks.

1. The user requests to connect to the wireless network through an access point.
2. The access point requests identification data (username) from the user, which is then sent to an authentication server.
3. The authentication server requests proof that the ID is valid.
4. The access point requests proof that the ID is valid from the user, in the form of a password.
5. The user supplies the access point with their password. The access point sends this back to the authentication server.
6. The server confirms the username and password are correct and passes this information on to the access point and user.
7. The user connects to the wireless network.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Authentication Protocols (Cont.)

Four protocols used with EAP to provide authentication for wireless networks are:

EAP-TLS
Requires Client Certificate: Yes
Requires Server Certificate: Yes
Easily Deployed: Difficult
Security: High

PEAP
Requires Client Certificate: No
Requires Server Certificate: Yes
Easily Deployed: Moderate
Security: Medium

EAP-TTLS
Requires Client Certificate: No
Requires Server Certificate: Yes
Easily Deployed: Moderate
Security: Medium

EAP-FAST
Requires Client Certificate: No
Requires Server Certificate: No
Easily Deployed: Easy
Security: Medium

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Mutual Authentication

Your wireless network and its sensitive data are susceptible to unauthorized access by hackers using a wireless connection. But what can you do to prevent an attack?

- **Rogue access points**: An access point is any hardware device that enables other wireless devices to connect to a wired network. Any device that has a wireless transmitter and hardwired interface to a network can potentially act as a rogue or unauthorized access point.

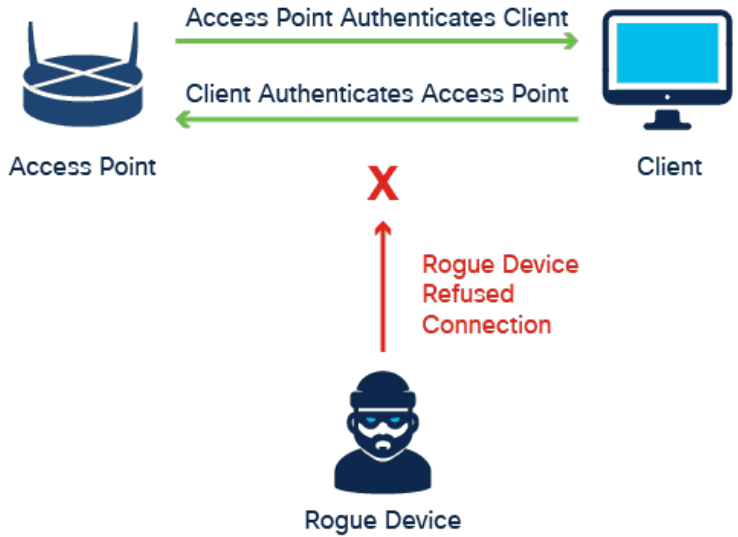
- The rogue access point will often imitate an authorized access point, allowing users to connect to the wireless network but potentially stealing their data or conducting other nefarious activity in the process.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Mutual Authentication (Cont.)

Preventing attacks: When you connect to a rogue access point, the imposter who set it up can request and copy data from your device.

Mutual authentication is two-way authentication that can prevent rogue access points. It is a process in which both entities in a communications link authenticate each other before they connect.



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Communication Methods

Mobile devices connect and communicate in the following ways:

Wi-Fi and Bluetooth

- Mobile devices can use wireless signals such as Wi-Fi and Bluetooth.

Near-field communication

- Near-field communication (NFC) allows contactless communication between devices. NFC chips use electromagnetic fields to enable contactless payments, meaning, for instance, that you simply hold your device close to a payment terminal to process payment.

Infrared

- Infrared (IR) provides short-range communication using an IR receiver. For example, IR allows you to control your television through your cell phone.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Communication Methods (Cont.)

USB communication

- The only type of communication on this list that is wired, USB communication allows you to use your smartphone for data or audio storage.
- USB connectivity also allows a mobile device to function as a modem or fax.
- You can connect a mobile device to forensic acquisition devices via the USB port if you need to gather information for an investigation.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Mobile Device Management

- A mobile device issued by an organization can contain both personal and organizational data — it can be either corporate-owned or corporate-owned personally enabled (COPE).

- An organization may also have a bring-your-own-device (BYOD) option. Security and data protection policies need to be applied when there is sensitive corporate information on a user's device.

Mobile device management methods can include:

Storage segmentation and containerization

- Storage segmentation and containerization allow you to separate personal and work content on a device. It provides an authenticated, encrypted area that separates sensitive company information from the user's personal data.

- Containerization also enables us to:
    - Isolate apps
    - Control app functions
    - Delete container information
    - Remotely wipe the device

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Mobile Device Management (Cont.)

Content management

- An organization needs to consider the security risks involved in using applications that share data — for example, Dropbox, Box, Google Drive, and iCloud. An identity-management security system can be used to control what data a user can access.

Application management

- Whitelisting allows you to **digitally sign** applications so that you can authorize which applications users can install. This helps to ensure that installed applications come from a trusted source.
- Authentication using strong passwords is a best practice for those applications that require user credentials.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Mobile Device Protections

Whether a mobile device is owned by the organization or is a personal device used for work, measures need to be put in place to keep it safe from cyber threats.

What are the risks?

Threats to mobile devices include:

- Theft
- Loss
- Unauthorized access
- Operating system risks
- Application risks
- Network risks

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Mobile Device Protections (Cont.)

- **Jailbreaking, rooting, and sideloading** are ways of bypassing a device's limitations to do things that the device is restricted from doing. Users may try to **jailbreak** (Apple devices) or **root** (Android devices) their device to run an app that is not authorized or available in the store.
- Jailbreaking removes the restriction that only Apple-authorized apps may run on the device.
- Rooting bypasses Android's security architecture to allow complete, administrative access to the device. Both pose a risk to the organization.
- Solutions are available that can detect a jailbroken or rooted device. A device is then marked as noncompliant and removed from the network or denied access to organizational apps.
- Third-party app stores can also pose a risk for organizations because the apps they provide access to have not been evaluated properly. **Sideloading** occurs when the user goes around the approved app settings to install unapproved apps. This is less invasive than jailbreaking or rooting, but it is still a risk.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Mobile Device Protections (Cont.)

What are the safeguards?
Safeguards against mobile device threats include the following:

- **Screen locks** require a password, PIN, or pattern to access the device.
- **Biometric authentication** uses a unique physical characteristic (fingerprint, face, iris, or voice).
- **Context-aware authentication** uses machine learning to determine access based on a user's normal behavior.
- **Remote wiping** deletes the device's data should the device be stolen or lost.
- **Full device encryption** can encrypt all data on a mobile device.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

GPS Tracking

- **Global Positioning System (GPS)** uses satellites and computers to determine the location of a device. GPS technology is a standard feature on smartphones and provides real-time position tracking that can typically pinpoint a location to within approximately 5 meters.
- Many cell phone apps use GPS tracking to track the phone's location.
- Push notifications sometimes use geolocation and geofencing - this enables local organizations to 'push' advertising messages based on a user's location settings. Unfortunately, increasingly savvy cyber attackers have started using push notifications to capture data.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

12.6 Cybersecurity Resilience

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

High Availability

- The term ‘high availability’ describes systems designed to avoid downtime as much as possible.
- The continuous availability of information systems is imperative, not only to organizations but to modern life, as we are all using and relying on computer and information systems more than ever before.
- High availability systems typically are based on three design principles: eliminating single points of failure, providing for reliable crossover, and detecting failures as they occur.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

High Availability (Cont.)

Eliminating Single Points of Failure

- The first principle that defines high availability systems starts with identifying all system devices and components whose failure would result in system-wide failure.

- Methods to eliminate single points of failure include replacing or removing hot stand-by devices, redundant components, and multiple connections or pathways.

Providing for Reliable Crossover

- Redundant power supplies, backup power systems and backup communications systems all provide for reliable crossover — the second design principle.

Detecting Failures as They Occur

- The third principle is active device and system monitoring to detect many types of events including system and device failures. Monitoring systems may even trigger the backup system in the case of failure.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Five Nines

- Every organization wants to be able to operate uninterrupted, even under extreme conditions, such as during an attack.

- One of the most popular high availability goals is often called ‘five nines.’ It gets its name from its aim to achieve an availability rate of 99.999%, which is five nines in a row. In practice, this means that downtime is less than 5.26 minutes per year.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Five Nines (Cont.)

Common steps taken to reach the five nines include:

Standardized Systems

- Systems standardization provides for systems that use the same components. As a result, parts inventories are easier to maintain and it is possible and easy to swap components, even during an emergency.
- In highly secure information system facilities, guards control access to the organization's sensitive areas.
- The benefit of using guards here is that they can adapt more than automated systems.
- Guards can learn and distinguish many different conditions and situations and make decisions on the spot.

Clustering

- Multiple devices grouped together provide a service that, to users, appears to be a single entity. If one device in a cluster fails, the other devices remain available and can step in.

Shared Component Systems

- Systems are built so that a complete system can stand in for one that failed.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Single Points of Failure

- Single points of failure are weak links in the chain that can cause disruption of the organization's operations.
  - A single point of failure is any part of the operation of the organization whose failure means complete failure of the entire system — in other words, if it fails, the entire system fails.
  - It can be a specific piece of hardware, a process, a specific piece of data, or even an essential utility.
  - Generally, the solution to a single point of failure is to modify the critical operation so that it does not rely on any single element.
  - The organization can also build redundant components into the operation to take over the process should one of these points fail.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

N+1 Redundancy

- N+1 redundancy helps ensure system availability in the event of a component failure. It means that components (N) need to have at least one backup component (+1).
- A good way to think about this is that a car has four tires (N) and a spare tire (+1) in the trunk in case of a flat.
- Although a system using N+1 architecture contains redundant equipment, it is not a fully redundant system.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

N+1 Redundancy (Cont.)

- In a network, N+1 redundancy means that the system design can withstand the loss of one of each component.
- The N refers to each different infrastructure component that is part of the system.
- The +1 is the additional component or system that is standing by, ready when needed.
- N+1 redundancy in a data center that consists of the above elements means that we have a server, a power supply, a switch and a router on standby, ready to come online if something happens to the main server, the main power source, switch, or router.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

RAID

How does it work?

- RAID takes data that is normally stored on a single disk and spreads it out among several drives. Except for RAID 0, if any single disk is lost, the user can recover data from the other disks where the data also resides.

- RAID can also increase the speed of data recovery as multiple drives will be faster retrieving requested data than one disk doing the same.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

RAID (Cont.)

RAID Data Storage

- A RAID solution can be either hardware-based or software-based. A hardware-based solution requires a specialized hardware controller on the system that contains the RAID drives, while software RAID is managed by utility software in the OS.

The following terms describe the various ways RAID can store data in the array of disks.

- **Mirroring** — Stores data, then duplicates and stores the same on a second drive.
- **Striping** — Writes data across multiple drives so that consecutive segments are stored on different drives.
- **Parity** — More precisely, striping with parity. After striping, checksums are generated to check that no errors exist in the striped data. These checksums are stored on a third drive.

Further RAID architectures exist, which mainly combine the above elements.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Spanning Tree

- Redundancy increases the availability of the infrastructure by protecting the network from a single point of failure, such as a failed network cable or a failed switch.

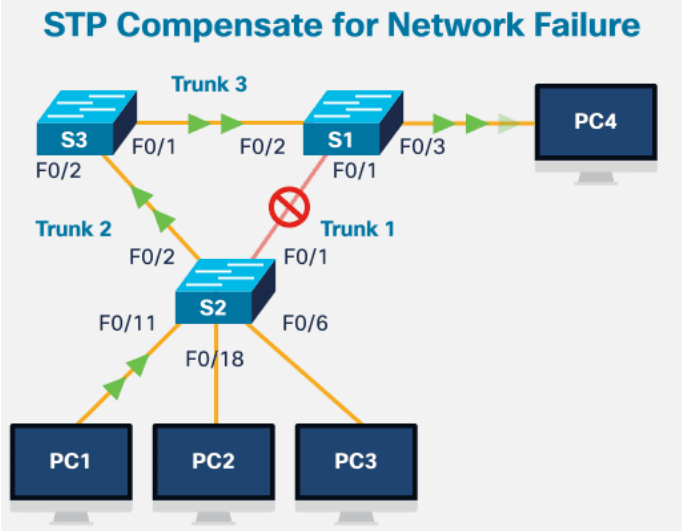
- The Spanning Tree Protocol (STP) addresses these issues. STP ensures that redundant physical links are loop-free and only one logical path runs between all destinations on the network.
  - Blocking the redundant paths is critical to preventing loops on the network. If a network cable or switch fails, STP recalculates the paths and unblocks the necessary ports to allow the redundant path to become active.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Spanning Tree (Cont.)

This animation shows the STP stages when a failure occurs.

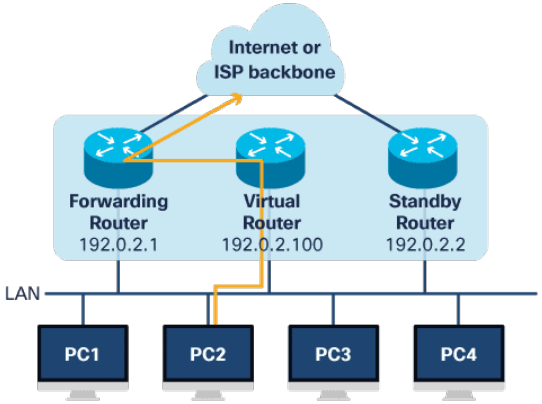
1. PC1 sends a broadcast out onto the network.
2. The trunk link between S2 and S1 fails, resulting in disruption of the original path.
3. S2 unblocks the previously blocked port for Trunk2 and allows the broadcast traffic to traverse the alternate path around the network, permitting communication to continue.
4. If the link between S2 and S1 comes back up, STP again blocks the link between S2 and S3.



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Router Redundancy

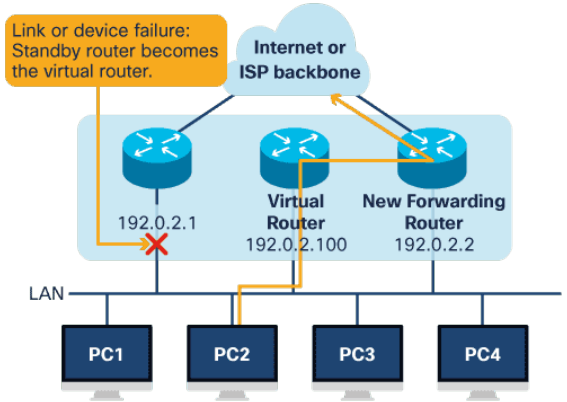
- The default gateway is typically the router that provides devices access to the rest of the network and/or to the internet.
  - If there is only one router serving as the default gateway, it is a single point of failure.
  - To avoid this, an organization can choose to install an additional standby router.



- A redundancy protocol determines which router should take the active role in forwarding traffic; the forwarding router or the standby router.
  - Each is configured with a physical IP address and a virtual router IP address.
  - End devices use the virtual IP address as the default gateway, which is 192.0.2.100.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Router Redundancy (Cont.)



- The forwarding router and the standby router use their physical IP addresses to send periodic messages. The purpose of these messages is to make sure both are still online and available.
- If the standby router stops receiving these periodic messages from the forwarding router, it realizes it is the only router available and assumes the forwarding role for itself.

- The ability of a network to dynamically recover from the failure of a device acting as a default gateway is known as first-hop redundancy.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Location Redundancy

An organization may also want to consider location redundancy, depending on its needs.

Synchronous Reputation:

- Synchronizes both locations in real time
- Requires high bandwidth
- Locations must be close together to reduce latency

Asynchronous Reputation:

- Not synchronized in real time but close to it
- Requires less bandwidth
- Sites can be further apart because latency is less of an issue

Point-in-Time-Replication:

- Updates the backup data location periodically, at certain points in time
- More bandwidth conservative because it does not require a constant connection

The correct balance between cost and availability will determine the correct choice for an organization.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Resilient Design

Resiliency is the name given to the methods and configurations used to make a system or network tolerant of failure.

- **Example:** A network having redundant links between switches running STP.
- Although STP does provide an alternate path through the network if a link fails, the switchover may not be immediate if the configuration is not optimal, so these redundant links together with STP provide more resiliency.

- Routing protocols also provide resiliency, but fine-tuning can improve the switchover so that network users do not notice.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Resilient Design (Cont.)

Application Resilience is an application's ability to react to component problems while still functioning.

- Application errors or infrastructure failures can cause downtime, but an administrator will eventually need to shut down applications for patching, version upgrades, or to deploy new features.
- Achieving resiliency of application infrastructure means avoiding losing customers, employee morale, or business due to an application failure.
- There are three availability solutions to address application resilience.
  - **Fault tolerant hardware**: A system designed by building multiples of all critical components into the same computer.
  - **Cluster architecture**: A group of servers acting like a single system.
  - **Backup and restore**: Copying files for the purpose of being able to restore them if data loss occurs.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Resilient Design (Cont.)

IOS Resilience

- The Interwork Operating System (IOS) for Cisco routers and switches includes a resilient configuration feature.
  - It allows for faster recovery if someone maliciously or unintentionally reformats flash memory or erases the startup configuration file.
  - The feature maintains a secure working copy of the router IOS image file and a copy of the running configuration file.
  - The user cannot remove these secure files, also known as the primary bootset.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

System and Data Backups

- An organization can lose data if cybercriminals steal it, if equipment fails, or if a disaster or other error occurs, so it's important to back up data regularly.
- A data backup stores a copy of the information from a computer to backup media. When such media is removable, the operator then stores this backup media in a safe place.
- Backing up data is one of the most effective ways of protecting against data loss. If the hardware fails, the user can restore the data from the backup once the system is functional again, or even when moving to a new system.
- A sound security policy should include regular data backups. Backups are usually stored off-site to protect the data if anything happens to the main facility.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

System and Data Backups (Cont.)

Additional considerations for data backups include:

Frequency

- Backups can take a long time. Sometimes, it is easier to make a full backup monthly or weekly and then do frequent partial backups of any data that has changed since the last full backup. However, having many partial backups increases the amount of time needed to restore the data.

Storage

- For extra security, transport backups to an approved off-site storage location on a daily, weekly, or monthly rotation, as required by the security policy.

Security

- Protect backups with passwords. The operator will enter the password before restoring the data from the backup media.

Validation

- Always validate backups to ensure the integrity of the data.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Designing High Availability Systems

High availability incorporates three major principles to achieve the goal of uninterrupted access to data and services.

Elimination or Reduction of Single Points of Failure

- It is important to understand the ways to address a single point of failure. A single point of failure can be a central router or switch, a network service, and even a highly skilled IT staff member.
- What makes these single points of failure is the fact that a loss or failure of this system, process, or person would have a very disruptive impact on the entire system, which should be avoided.

- High availability clusters are one way to provide redundancy.
  - These clusters consist of a group of computers with identical configurations and access to the same shared storage.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Designing High Availability Systems (Cont.)

Fault Tolerance

- Fault tolerance enables a system to continue to operate if one or more of its components fail.
  - Data mirroring is one example of fault tolerance.

System Resiliency

- System resiliency refers to the capability to maintain availability of data and operational processing despite attacks or disrupting events.
  - Generally, this requires redundant systems, in terms of both power and processing, so that should one system fail, the other can take over operations without any break in service.
  - System resiliency is more than hardened devices; it requires that both data and services be available, even when under attack.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Power

- A critical issue in protecting information systems is electrical power systems and power considerations. A continuous supply of electrical power is essential for today's massive server and data storage facilities.

Here are some general rules in building effective electrical supply systems:

- Data centers should be on a different power supply from the rest of the building.
- Use redundant power sources — two or more feeds coming from two or more electrical substations.
- Implement power conditioning.
- Backup power systems are often required.
- Uninterruptible power supply (UPS) should be available to gracefully shut down systems.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Power (Cont.)

Some standard terms linked to electrical power system events include:

Power Excess

- Spike: momentary high voltage
- Surge: prolonged high voltage

Power Loss

- Fault: momentary loss of power
- Blackout: complete loss of power

Power Degradation

- Sag/dip: momentary low voltage
- Brownout: prolonged low voltage
- Inrush current: initial surge of power

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Heating, Ventilation and Air Conditioning (HVAC)

HVAC systems are critical to the safety of people and information systems in an organization's facilities. When designing modern IT facilities, these systems play a very important role in the overall stability and security.

- **HVAC systems** control the ambient environment, including the temperature, humidity, and airflow. This must be managed along with data components such as hardware, cabling, data storage, fire protection, physical security systems and power, and their needs.

- **A product specifications document**
  - Almost all physical computer hardware comes with environmental requirements that include acceptable temperature and humidity ranges.
  - Environmental requirements are detailed in product specifications documentation and/or physical planning guides.
  - It is critical to observe these environmental requirements to prevent system failures and extend the life of IT systems.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Heating, Ventilation and Air Conditioning (HVAC) (Cont.)

HVAC system contractor

- Commercial HVAC systems and other building management systems now connect to the internet for remote monitoring and control.
- But recent events have shown such ‘smart’ systems also raise big security issues, as they are accessed and managed by HVAC system contractors or third-party vendors.

Risks to the organization's security

- Because HVAC technicians need to be able to find information quickly, crucial data tends to be stored in many different places, making it accessible to even more people.
- This allows a wide network of individuals, including even associates of contractors, to gain access to the HVAC system.
- But the more people have access, the less secure these systems are, while their interruption can pose considerable risk to the organization's security.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Managing Threats to Physical Facilities

Organizations can implement various measures to manage threats to the physical facilities.

For example:

- Access Control and Closed-Circuit TV (CCTV - Video Surveillance) coverage at all entrances
- Policies and procedures for guests visiting the facility
- Building security testing, including using both digital and physical means to covertly gain access
- Badge encryption for entry access
- Disaster recovery planning
- Business continuity planning
- Regular security awareness training
- Asset tagging system

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

12.7 Embedded and Specialized Systems

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Threats to Key Industry Sectors

- Over the last decade, cyber-attacks like Stuxnet proved that malware attacks could successfully destroy or interrupt critical infrastructures.
  - The Stuxnet worm targeted Supervisory Control And Data Acquisition (SCADA) systems used to control and monitor industrial processes. SCADA and other Industrial Control Systems (ICSs) are used in manufacturing, production, energy, and communications systems.

How can cyber-attacks like these impact industry sectors and what action can be taken to prevent such attacks from occurring?

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Threats to Key Industry Sectors (Cont.)

Stuxnet: A cyber-attack like this could bring down or interrupt vital facilities like telecommunications, transportation systems or electrical power plants. It could also interrupt the financial services sector.

- Environments that use SCADA are vulnerable.
- When the SCADA architecture was first being developed, designers did not connect it to the traditional IT environment and the Internet.
- Therefore, they did not properly consider cybersecurity during the development phase of these systems.
- To prevent attacks on these systems, you should segregate internal and external networks to separate the SCADA network from the organization's LAN.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Emergence of the Internet of Things

- The Internet of Things (IoT) is the collection of technologies that enable various devices to connect to the Internet.
- IoT technologies enable people to connect billions of devices, such as cars, industrial machines, robots, appliances, locks, motors and entertainment devices, to name just a few.
- With the emergence of IoT, there is much more data to be managed and secured.
- IoT devices greatly expand the cyber attack surface.
- In the IoT, thousands of new devices require access to networks to submit data and be managed and operated.
- Internet-connected smart devices have been infected with malware and used to launch some of the largest DDoS attacks in history.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Embedded Systems

- Embedded systems capture, store and access data. They pose unique security challenges due to their widespread adoption by both the corporate and the consumer world. They are used in smart TVs, HVAC control systems, medical devices, and even automobiles.

Why are embedded systems vulnerable to attack?

- Attacks against embedded systems exploit security vulnerabilities in the software and hardware components.
  - They are susceptible to timing attacks, whereby attackers discover vulnerabilities by studying how long it takes the system to respond to different inputs.
  - A timing attack is considered a side-channel attack.
    - This type of attack is based on information gained from the implementation of a system, rather than on weaknesses in the software.
    - Timing information, power consumption, electromagnetic leaks, or even sound can be that source of information.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Embedded Systems (Cont.)

How can embedded systems be protected?

- One technique is to use System on Chip (SoC) technology. SoC technology is a Small Form Factor (SFF) hardware module — customer-grade examples include devices such as Raspberry Pi and Arduino. These devices are single-board computers that can be implemented using a Field-Programmable Gate Array (FGPA), an integrated circuit that can be programmed or modified in the field. This means that the user can make changes after deploying the device.

- These devices have good processing power delivered in a small footprint.
- SoC integrates a microcontroller, an application or microprocessor, and peripherals such as a GPU, a Wi-Fi module or a coprocessor.
- Many of these SoC devices have poor authentication and/or they cannot be upgraded or patched.
    - Due to the nature of these devices, a level of implied trust is necessary since there is no formal program in place to verify security controls.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Internet of Things (IoT)

- The deployment and use of intelligent devices and sensors is one of the fastest growing sectors of information technology. The computer industry brands this sector as the Internet of Things (IoT).

- Businesses and consumers use IoT devices to automate processes, monitor environmental conditions, and alert the user of adverse conditions.
  - Most IoT devices connect to a network via wireless technology.
  - These include cameras, door locks, proximity sensors, lights, and other sensors used to collect information about an environment or the status of a device.
  - Some manufacturers use IoT sensors to inform users that parts need to be replaced, components are failing, or supplies are running out.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Internet of Things (IoT) (Cont.)

- Organizations use IoT devices to track inventory, vehicles and personnel.
- IoT devices contain geospatial sensors.
  - A user can globally locate, monitor and control environmental variables such as temperature, humidity, and lighting.
  - IoT applications use a Real-Time Operating System (RTOS), a small operating system that allows for the rapid switching of tasks that focus on timing rather than throughput.

- The IoT industry poses a tremendous challenge to information security professionals because many IoT devices capture and transmit sensitive information.
- Vulnerabilities associated with RTOS include code injection, DoS attacks, and priority inversion (where a higher priority task is pre-empted by a lower priority task).

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Securing IoT Devices

- Using an IoT scanner such as Shodan is an easy way to tell whether a home automation device is vulnerable to attack.
- IoT devices communicate using short-range, medium-range, or long-range methods and include cellular (4G, 5G), radio, and Zigbee.
- Zigbee is a wireless set of protocols for Wireless Personal Area Networks (WPANs).

- To secure IoT devices:
  - Secure the wireless network.
  - Know exactly which devices are communicating on your network.
  - Know what each of the IoT devices on your network does.
  - Install security software on devices where possible.
  - Secure smartphones and mobile apps used to communicate with IoT devices.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

VoIP Equipment

VoIP uses the internet to make and receive phone calls.

What equipment do you need?
You need an internet connection and a phone for VoIP.

- Several options are available for the phone set:
  - A traditional phone with an adapter (The adapter acts as a hardware interface between a traditional, analog phone and a digital VoIP line.)
  - A VoIP-enabled phone
  - VoIP software installed on a computer

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

VoIP Equipment (Cont.)

Is VoIP secure?

- Most consumer VoIP services use the internet for phone calls. VoIP security is only as reliable as the underlying network security. Cybercriminals target these systems to gain access to free phone services, to eavesdrop on phone calls, or to affect performance and availability.

How can you protect your VoIP service?

Implement the following countermeasures to secure VoIP:

- Encrypt voice message packets to protect against eavesdropping.
- Use SSH to protect gateways and switches.
- Change all default passwords.
- Use an intrusion detection system to detect attacks such as ARP poisoning.
- Use strong authentication to mitigate registration spoofing (cybercriminals routing all incoming calls for the victim to themselves), proxy impersonating (tricking the victim into communicating via a rogue proxy set up by the cybercriminals), and call hijacking (intercepting and rerouting calls to a different path before reaching their destination).
- Implement firewalls that recognize VoIP to monitor streams and filter abnormal signals.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Special-Purpose Embedded Systems

- Embedded systems work in a variety of industries. You can find special-purpose embedded devices in sectors such as the medical, automotive, and aviation sectors.

Medical devices

- Devices such as pacemakers, insulin pumps, medical implants, and defibrillators are capable of wireless connectivity, remote monitoring, and Near-Field Communication (NFC).

- Vulnerabilities in these medical devices can lead to patient safety issues, medical record leaks, or the risk of granting access to the network to cybercriminals, who will move through it in search of a target.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Special-Purpose Embedded Systems (Cont.)

Automotive

- In-vehicle systems produce and store the data necessary for the operation of the vehicle along with its maintenance, safety protection, and emergency contact transmission.
- Typically, a wireless interface connects to the Internet and to a diagnostic interface on board.
- Many vehicles record speed, location, and braking maneuvers, and can then send the collected data to the driver's insurance company.
- Risks to in-vehicle communications include unauthorized tracking, wireless jamming, and spoofing.
- To secure in-vehicle systems, implement the following countermeasures:
  - Secure system software design practices
  - Basic encryption for all communication between controllers
  - Firewall implementation

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Special-Purpose Embedded Systems (Cont.)

Aviation

- An aircraft has many embedded control systems such as its flight control system and communication system. Security issues include the use of hard-coded logon credentials, insecure protocols and backdoors.

- In the same category, Unmanned Aerial Vehicles (UAVs), more commonly called drones, have been used in military, agricultural and cartography applications, among others.

- Drones are susceptible to hijacking, Wi-Fi attacks, GPS spoofing attacks, jamming and deauthentication attacks, which can allow an attacker to intercept or disable a drone and access its data.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Deception Technologies

- Organizations use deception technologies to distract attackers from production networks. They also use them to learn an attacker's methods and to warn of potential attacks that could be launched against the network. Deception adds a fake layer to the organization's infrastructure.

- A **honeypot** is a decoy system that is configured to mimic a server in the organization's network. It is purposefully left exposed, to lure attackers. When an attacker goes after the honeypot, their activities are logged and monitored for later review. The honeypot distracts the attacker from the organization's real network resources.

- An organization might even create a **honeynet**, a collection of honeypots, to mimic its network and distract attackers. Meanwhile, honeyfiles are dummy files that attract an attacker but do not contain any real information.

- A **DNS sinkhole** prevents the resolution of hostnames for specified URLs and can push users away from malicious resources.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

PT Video - Implement Physical Security with IoT Devices

In this Packet Tracer you will learn how to:

- Connect IoT devices to the network.
- Add IoT devices to the registration server.
- Explore IoT security device functionality.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Packet Tracer - Implement Physical Security with IoT Devices

In this Packet Tracer activity, you will complete the following objectives:

- Part 1: Connect IoT Devices to the Network
- Part 2: Add IoT Devices to the Registration Server
- Part 3: Explore IoT Security Device Functionality

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

12.8 System and Network Defense Summary

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What Did I Learn in this Module?

Physical security:

- Barricades or fencing are the two most common types of physical security.
- Biometrics are the physiological or behavioral characteristics of an individual.
- Biometric authentication systems can include measurements of the face, fingerprint, hand geometry, iris, retina, signature, and voice.
- The most common metric to describe the overall accuracy of a biometric authentication system is the Crossover Error Rate (CER).
- RFID asset tags can track any asset that physically leaves a secure area.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What Did I Learn in this Module? (Cont.)

Application Security:

- To maintain security at all stages of application development, follow a process that includes: developing and testing, staging and production, and provisioning and deprovisioning.
- When coding applications, developers use techniques to validate that all security requirements have been met including: normalization, stored procedure, obfuscation and camouflage, code reuse, and SDKs.
- A validation rule checks that data falls within the parameters defined by the database designer. This helps to ensure the completeness, accuracy, and consistency of data.
- The integrity check performs a hash function to take a snapshot of data and then uses this snapshot to ensure data has remained unchanged.
- A checksum is an example of a hash function.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What Did I Learn in this Module? (Cont.)

Network Hardening Services and Protocol:

- Cybercriminals use vulnerable network services to attack a device, or to use it as part of an attack.
- A port scanner sends a message to each port and waits for a response, which indicates how the port is used and whether it is open.
- DHCP uses a server to assign an IP address and other configuration information to network devices.
- DNSSEC uses digital signatures to strengthen authentication and protect against threats to the DNS.
- The ping command is a network utility that uses ICMP to test the reachability of a host on a network.
- NTP allows network devices to synchronize their time settings with an NTP server.
- Secure Shell (SSH) is a protocol that provides a secure (encrypted) remote connection to a device. Telnet is an older protocol that uses unsecure plaintext when authenticating a device and transmitting data.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What Did I Learn in this Module? (Cont.)

Network Hardening: Segmentation:

- VLANs provide a way to group devices within a LAN and on individual switches.
- VLANs are based on logical connections, while LANs are based on physical connections. Individual ports on a switch can be assigned to a specific VLAN.
- A DMZ is a small network between a trusted private network and the internet.
- Web servers and mail servers are usually placed within the DMZ to allow users to access an untrusted network, such as the internet, without compromising the internal network.
- Most networks have two to four zones of risk: the trusted private LAN, the DMZ, the internet, and an extranet.
- To protect its network, an organization can implement a Zero Trust model.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What Did I Learn in this Module? (Cont.)

Hardening Wireless and Mobile Devices:

- WEP was the first security protocol used for wireless networks.
- Open system authentication is where any wireless device can connect to the wireless network.
- Shared key authentication provides mechanisms to authenticate and encrypt data between a wireless client and AP or wireless router.
- EAP is an authentication framework used in wireless networks and includes EAP-TLS, PEAP, EAP-TTLS and EAP-FAST.
- Mutual authentication is two-way authentication in which both entities in a communications link authenticate each other before they connect.
- NFC allows contactless communication between devices.
- IR provides short-range communication using an IR receiver.
- USB communication is the only type of communication on this list that is wired.
- Jailbreaking, rooting and sideloading are ways of bypassing a device's limitations to do things that the device is restricted from doing.
- Safeguards include screen locks, biometric authentication, context-aware authentication, remote wiping, and full device encryption.
- GPS uses satellites and computers to determine the location of a device.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential