

Module 21: Cryptography

Instructor Materials

CyberOps Associate v1.0

Module 21: Cryptography

CyberOps Associate v1.0

Module Objectives

Module Title: Public Key Cryptography

Module Objective: Explain how the public key infrastructure (PKI) supports network security.

Topic Title	Topic Objective
Integrity and Authenticity	Explain the role of cryptography in ensuring the integrity and authenticity of data.
Confidentiality	Explain how cryptographic approaches enhance data confidentiality.
Public Key Cryptography	Explain public key cryptography.
Authorities and the PKI Trust System	Explain how the public key infrastructure functions.
Applications and Impacts of Cryptography	Explain how the use of cryptography affects cybersecurity operations.

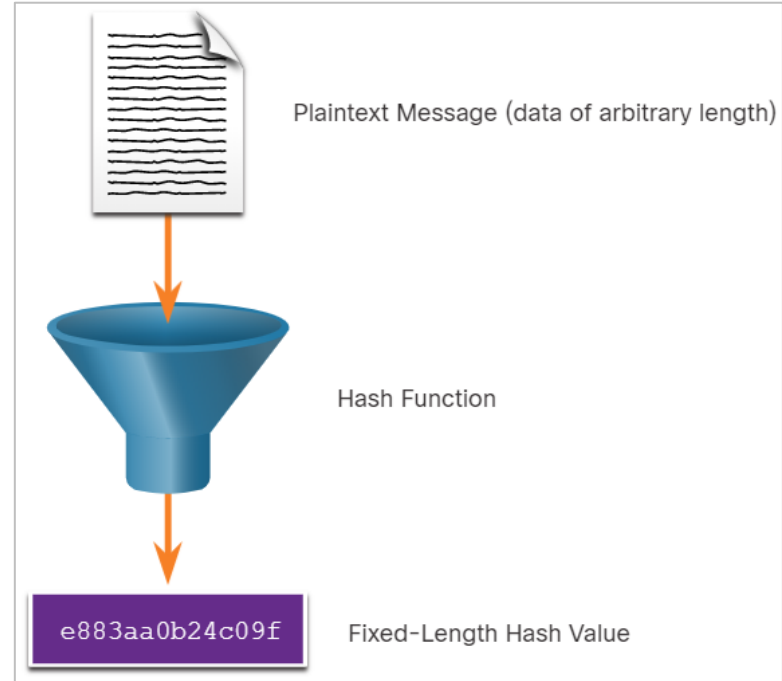
21.1 Integrity and Authenticity

Securing Communications

- Organizations must provide support to secure the data internally as well as externally.
- The four elements of securing communications are:
 - Data Integrity - Guarantees that the message was not altered.
 - Origin Authentication - Guarantees that the message is not a forgery and it actually comes from whom it states.
 - Data Confidentiality - Guarantees that only authorized users can read the message.
 - Data Non-Repudiation - Guarantees that the sender cannot repudiate, or refute, the validity of a message sent.

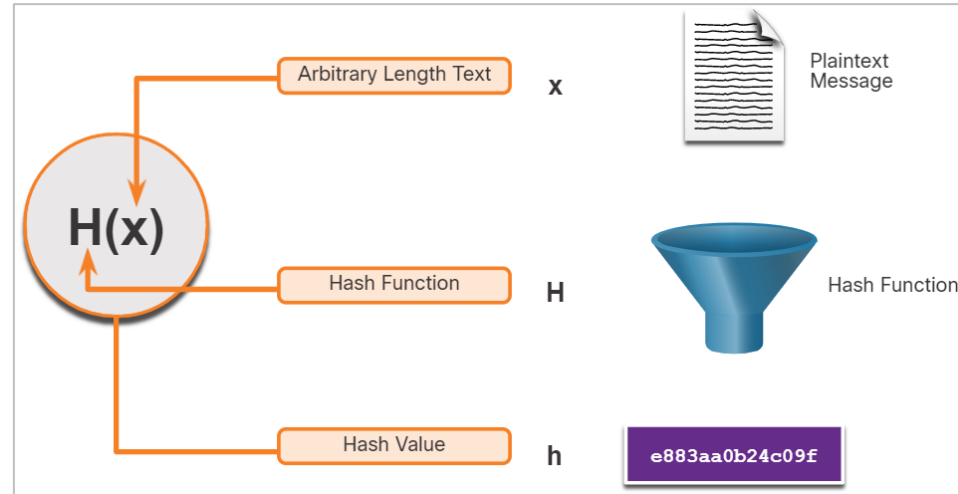
Cryptographic Hash Functions

- Hashes are used to verify and ensure data integrity.
- Hashing is based on a one-way mathematical function that is relatively easy to compute, but significantly harder to reverse.
- A hash function takes a variable block of binary data, called the message, and produces a fixed-length, condensed representation, called the hash.
- The resulting hash is also sometimes called the message digest, digest, or digital fingerprint.
- With hash functions, it is computationally infeasible for two different sets of data to come up with the same hash output.
- Every time the data is changed or altered, the hash value also changes.



Cryptographic Hash Operation

- Mathematically, the equation $h = H(x)$ is used to explain how a hash algorithm operates.
- As shown in the figure, a hash function H takes an input x and returns a fixed-size string hash value h .
- A cryptographic hash function should have the following properties:
 - The input can be any length.
 - The output has a fixed length.
 - $H(x)$ is relatively easy to compute for given x .
 - $H(x)$ is one way and not reversible.
 - $H(x)$ is collision free, meaning that two different input values will result in different hash values.

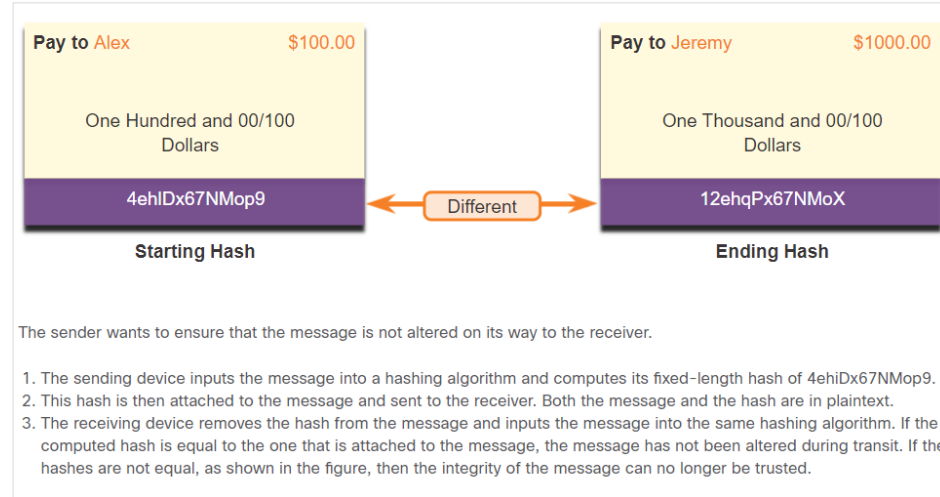


MD5 and SHA

- Hash functions are used to ensure the integrity of a message either accidentally or intentionally.
- In the figure, the sender is sending a \$100 money transfer to Alex. The sender wants to ensure that the message is not altered on its way to the receiver.

There are four well-known hash functions:

- **MD5 with 128-bit digest** - A one-way function that produces a 128-bit hashed message. MD5 is a legacy algorithm.
- **SHA-1** - Very similar to the MD5 hash functions. SHA-1 creates a 160-bit hashed message and is slightly slower than MD5.
- **SHA-2** - If you are using SHA-2, then SHA-256, SHA-384, and SHA-512 algorithms should be used.
- **SHA-3** - Next-generation algorithms and should be used whenever possible.



MD5 and SHA (Contd.)

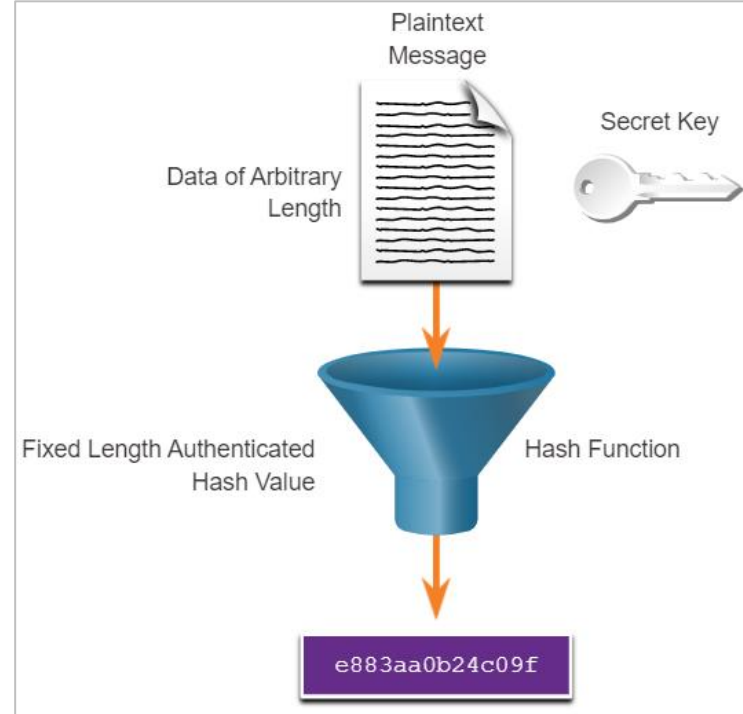
- While hashing can be used to detect accidental changes, it cannot be used to guard against deliberate changes that are made by a threat actor.
- There is no unique identifying information from the sender in the hashing procedure.
- This means that anyone can compute a hash for any data, as long as they have the correct hash function.
- Therefore, hashing is vulnerable to man-in-the-middle attacks and does not provide security to transmitted data. To provide integrity and origin authentication, something more is required.
- **Note:** *Hashing algorithms only protect against accidental changes and does not protect the data from changes deliberately made by a threat actor.*

Origin Authentication

- To add origin authentication and integrity assurance, use a keyed-hash message authentication code (HMAC).
- HMAC uses an additional secret key as input to the hash function.
- **Note:** *Other Message Authentication Code (MAC) methods are also used. However, HMAC is used in many systems including SSL, IPsec, and SSH.*

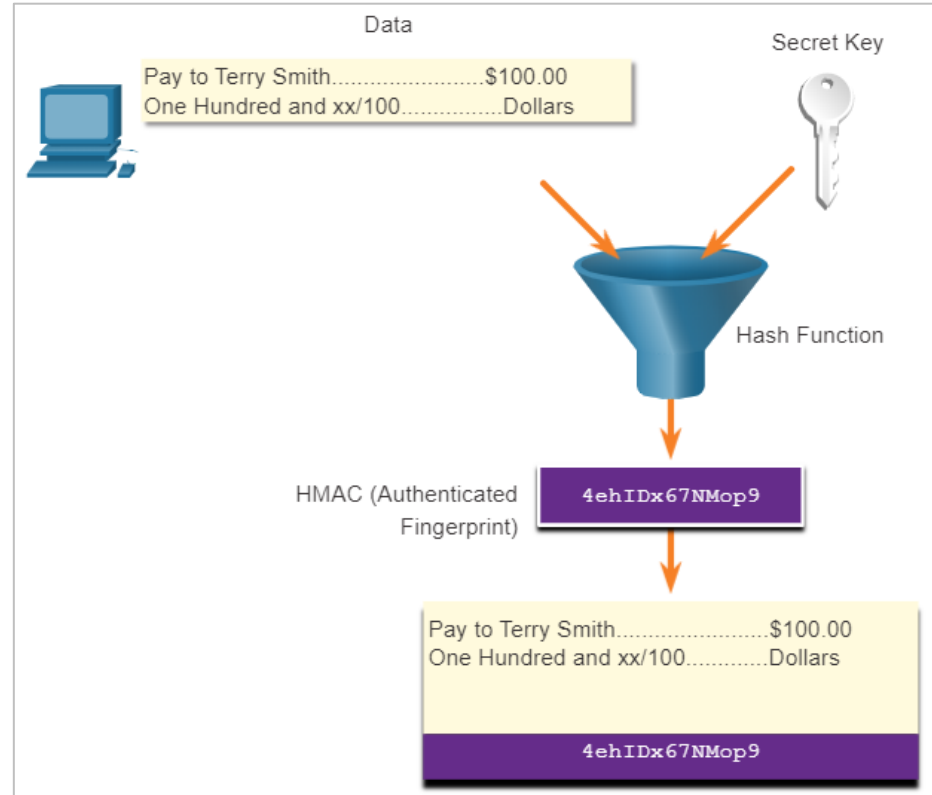
Origin Authentication (Contd.)

- HMAC Hashing Algorithm
- An HMAC is calculated using any cryptographic algorithm that combines a cryptographic hash function with a secret key.
- Only the sender and the receiver know the secret key, and the output of the hash function depends on the input data and the secret key.
- Only parties who have access to that secret key can compute the digest of an HMAC function.
- If two parties share a secret key and use HMAC functions for authentication, a properly constructed HMAC digest of a message that a party has received indicates that the other party was the originator of the message.



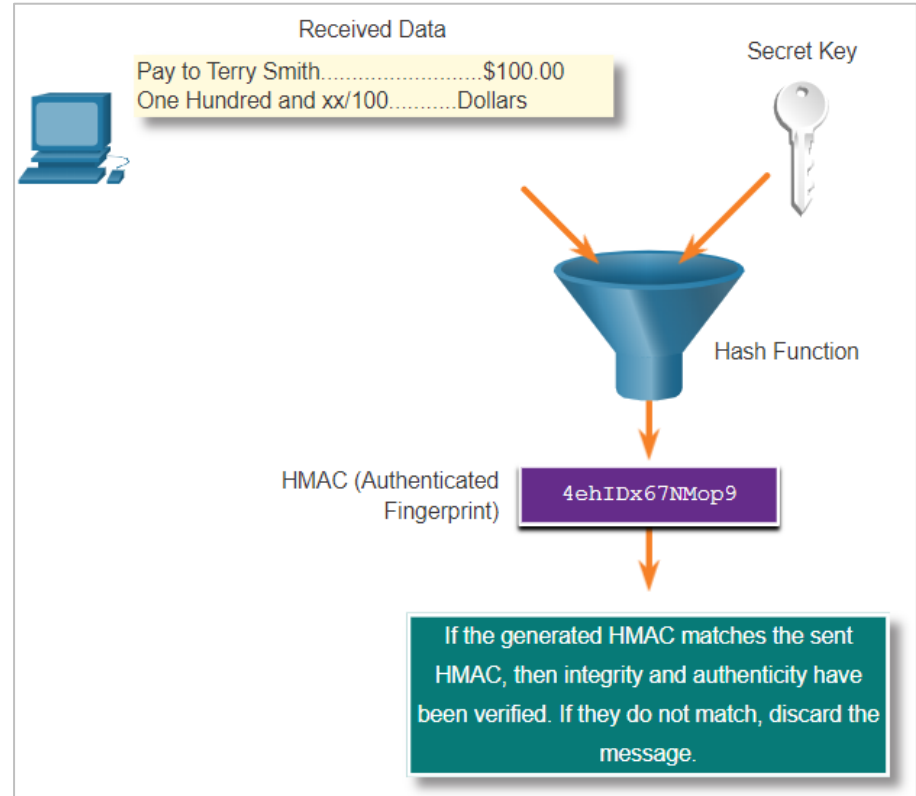
Origin Authentication (Contd.)

- Creating the HMAC Value
- As shown in the figure, the sending device inputs data into the hashing algorithm and calculates the fixed-length HMAC digest.
- This authenticated digest is then attached to the message and sent to the receiver.



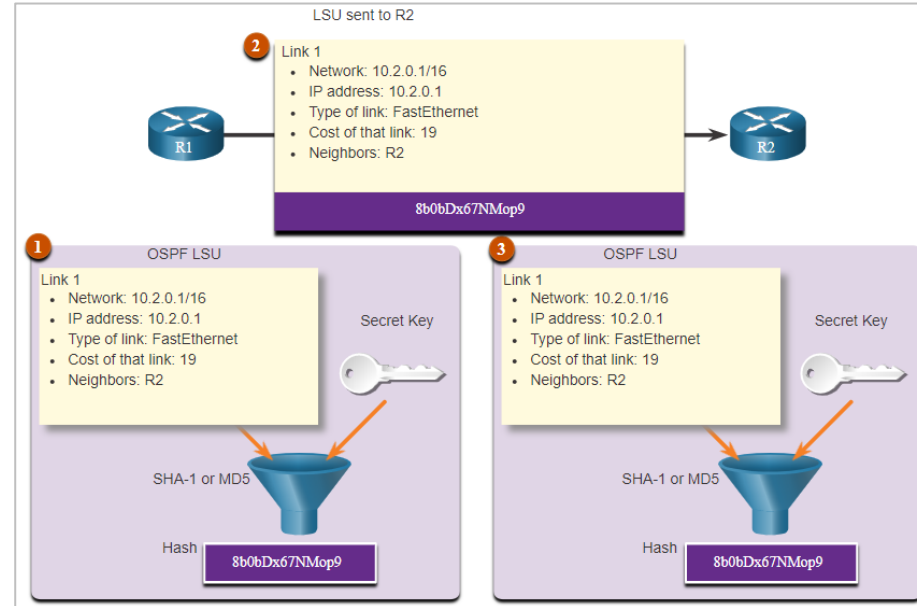
Origin Authentication (Contd.)

- Verifying the HMAC Value
- In the figure, the receiving device removes the digest from the message and uses the plaintext message with its secret key as input into the same hashing function.
- If the digest that is calculated by the receiving device is equal to the digest that was sent, the message has not been altered.
- Additionally, the origin of the message is authenticated because only the sender possesses a copy of the shared secret key. The HMAC function has ensured the authenticity of the message.



Origin Authentication (Contd.)

- Cisco Router HMAC Example
- In the figure, HMACs are used by Cisco routers that are configured to use Open Shortest Path First (OSPF) routing authentication.
- R1 is sending a link state update (LSU) regarding a route to network 10.2.0.0/16:
 - R1 calculates the hash value using the LSU message and the secret key.
 - The resulting hash value is sent with the LSU to R2.
 - R2 calculates the hash value using the LSU and its secret key. R2 accepts the update if the hash values match. If they do not match, R2 discards the update.



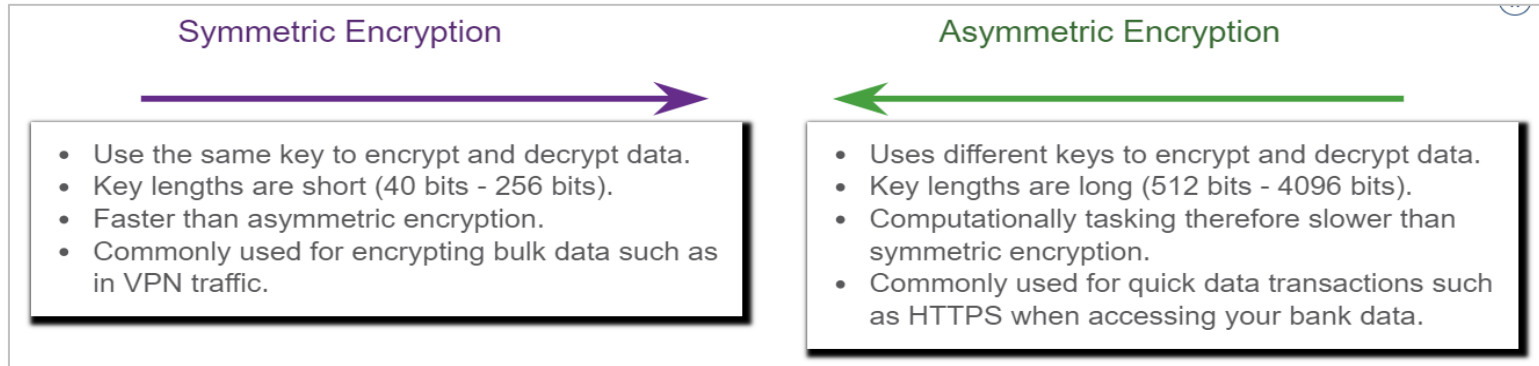
Lab – Hashing Things Out

- In this lab, you will complete the following objectives:
- Creating Hashes with OpenSSL
- Verifying Hashes

21.2 Confidentiality

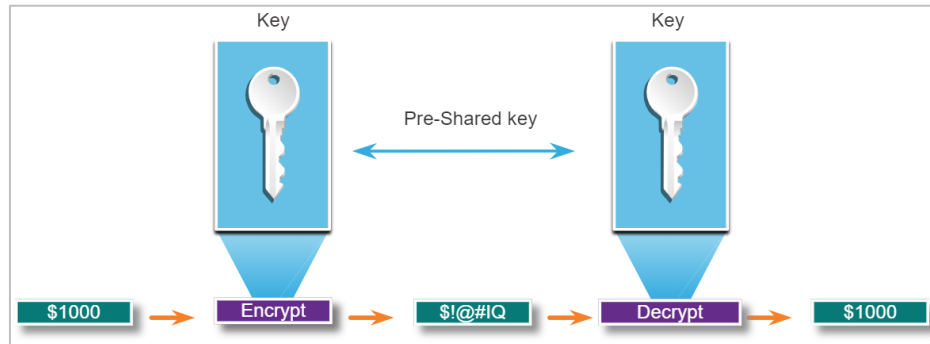
Data Confidentiality

- There are two classes of encryption used to provide data confidentiality; asymmetric and symmetric. These two classes differ in how they use keys.
- Symmetric encryption algorithms such as Data Encryption Standard (DES), 3DES, and Advanced Encryption Standard (AES) are based on the premise that each communicating party knows the pre-shared key.
- Data confidentiality can also be ensured using asymmetric algorithms, including Rivest, Shamir, and Adleman (RSA) and the public key infrastructure (PKI).
- The figure highlights some differences between symmetric and asymmetric encryption.



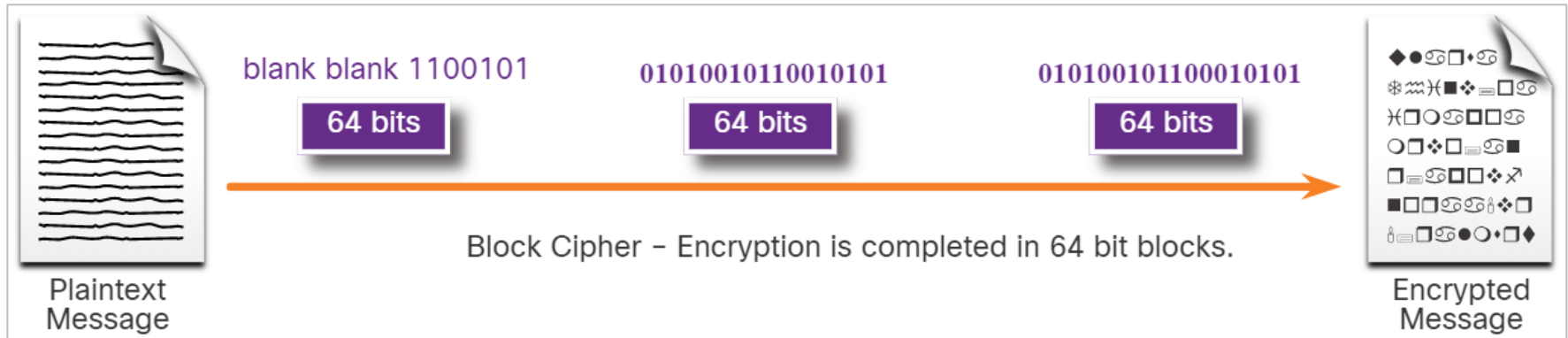
Symmetric Encryption

- Symmetric algorithms use the same pre-shared key (secret key) to encrypt and decrypt data.
- Symmetric encryption algorithms are commonly used with VPN traffic because they use less CPU resources than asymmetric encryption algorithms.
- When using these algorithms, the longer the key, the longer it will take for someone to discover the key.
- Most encryption keys are between 112 and 256 bits. Use a longer key for more secure communications.
- Symmetric encryption algorithms are sometimes classified as a block cipher or a stream cipher.



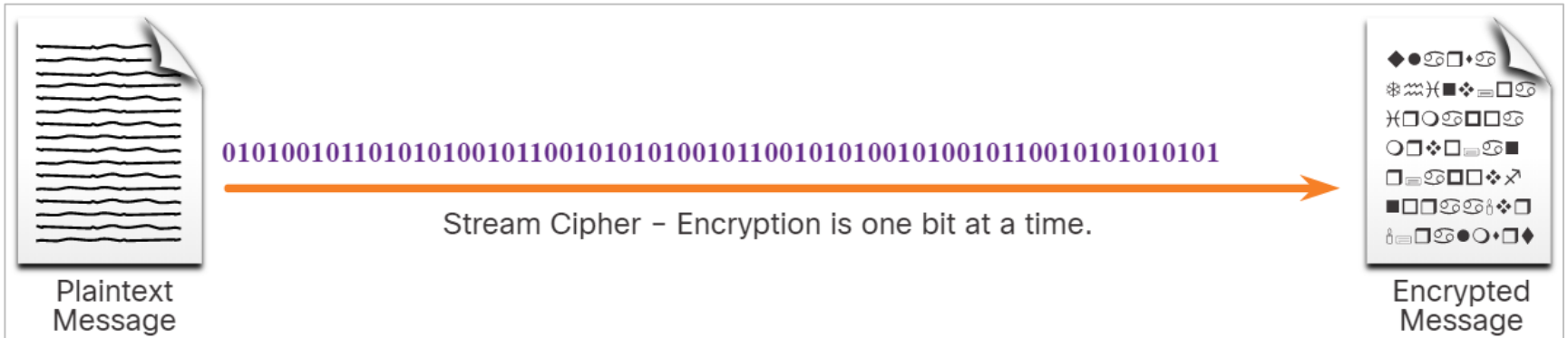
Symmetric Encryption (Contd.)

- Block Ciphers
- Block ciphers transform a fixed-length block of plaintext into a common block of ciphertext of 64 or 128 bits.
- Common block ciphers include DES with a 64-bit block size and AES with a 128-bit block size.



Symmetric Encryption (Contd.)

- Stream Ciphers
- Stream ciphers encrypt plaintext one byte or one bit at a time.
- Stream ciphers are basically a block cipher with a block size of one byte or bit.
- Stream ciphers are typically faster than block ciphers because data is continuously encrypted.
- Examples include RC4 and A5 which is used to encrypt GSM cell phone communications.



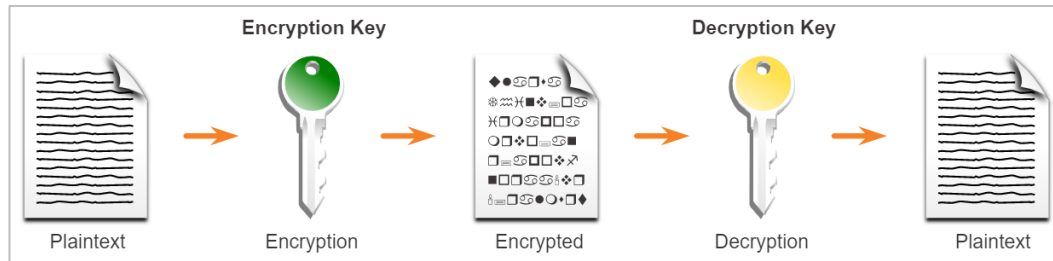
Symmetric Encryption (Contd.)

- Well-known symmetric encryption algorithms are described in the table.

Symmetric Encryption Algorithms	Description
Data Encryption Standard (DES)	This is a legacy algorithm. It uses a short key length that makes it insecure.
3DES (Triple DES)	This is the replacement for DES and repeats the DES algorithm three times. It should be avoided as it is scheduled to be retired in 2023. If implemented, use very short key lifetimes.
Advanced Encryption Standard (AES)	It offers combinations of 128-, 192-, or 256-bit keys to encrypt 128, 192, or 256 bit-long data blocks.
Software-Optimized Encryption Algorithm (SEAL)	It is a stream cipher that uses a 160-bit encryption key and has a lower impact on the CPU compared to other software-based algorithms.
Rivest ciphers (RC) series algorithms	RC4 is a stream cipher that was used to secure web traffic. It has been found to have multiple vulnerabilities which have made it insecure. RC4 should not be used.

Asymmetric Encryption

- Asymmetric algorithms, also called public-key algorithms, are designed in a way that the encryption and the decryption keys are different.
- Asymmetric algorithms use a public key and a private key. Both keys are capable of the encryption process, but the complementary paired key is required for decryption.
- The process is also reversible. Data that is encrypted with the public key requires the private key to decrypt.
- Asymmetric algorithms achieve confidentiality and authenticity by using this process.
- Asymmetric encryption can use key lengths between 512 to 4,096 bits.
- Asymmetric algorithms are substantially slower than symmetric algorithms.



Asymmetric Encryption (Contd.)

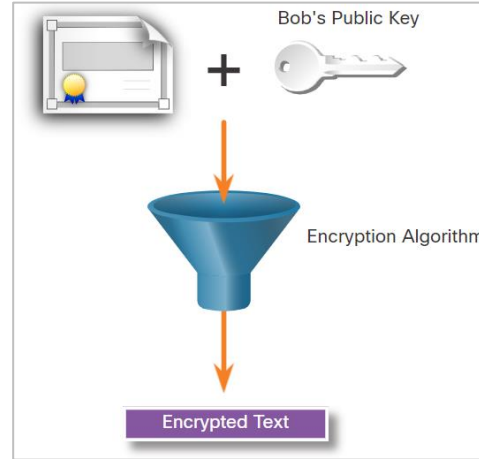
- Common examples of asymmetric encryption algorithms are described in the table.

Asymmetric Encryption Algorithms	Key Length	Description
Diffie-Hellman (DH)	512, 1024, 2048, 3072, 4096	This algorithm allows two parties to agree on a key that they can use to encrypt messages they want to send to each other. The security depends on the assumption that it is easy to raise a number to a certain power, but difficult to compute which power was used, given the number and the outcome.
Digital Signature Standard (DSS) and Digital Signature Algorithm (DSA)	512 – 1024	It specifies DSA as the algorithm for digital signatures. DSA is a public key algorithm based on the ElGamal signature scheme. Signature creation speed is similar to RSA, but is 10 to 40 times slower for verification.
Elliptic curve techniques	224 or higher	Elliptic curve cryptography can be used to adapt many cryptographic algorithms, such as Diffie-Hellman or ElGamal. The main advantage of elliptic curve cryptography is that the keys can be much smaller.

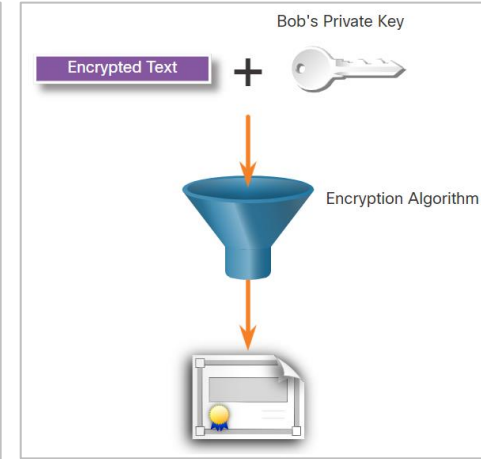
Asymmetric Encryption - Confidentiality

- Asymmetric algorithms are used to provide confidentiality without pre-sharing a password.
- The confidentiality objective of asymmetric algorithms is initiated when the encryption process is started with the public key.
- The process can be summarized using the formula: Public Key (Encrypt) + Private Key (Decrypt) = Confidentiality
- When the public key is used to encrypt data, the private key must be used to decrypt data.
- Only one host has the private key; therefore, confidentiality is achieved.

Example: Data exchange between Bob and Alice



Alice acquires and uses Bob's public key to encrypt a message and then send it to Bob.



Bob decrypts the message with the private key and as he is the only one with the private key, confidentiality is achieved.

Asymmetric Encryption - Authentication

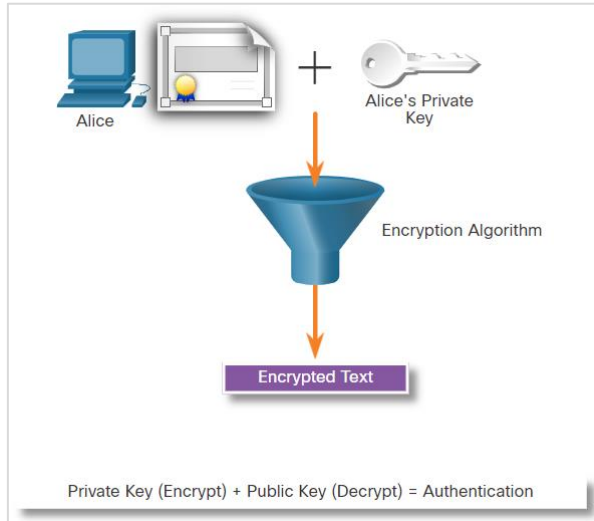
- The authentication objective of asymmetric algorithms is initiated with the private key encryption process.
- The process can be summarized using the formula: Private Key (Encrypt) + Public Key (Decrypt) = Authentication
- When the private key is used to encrypt the data, the corresponding public key must be used to decrypt the data.
- Because only one host has the private key, only that host could have encrypted the message, providing authentication of the sender.
- When a host successfully decrypts a message using a public key, it is trusted that the private key encrypted the message, which verifies who the sender is. This is a form of authentication.

Asymmetric Encryption - Authentication (Contd.)

- Let's see how the private and public keys can be used to provide authentication to the data exchange between Bob and Alice.

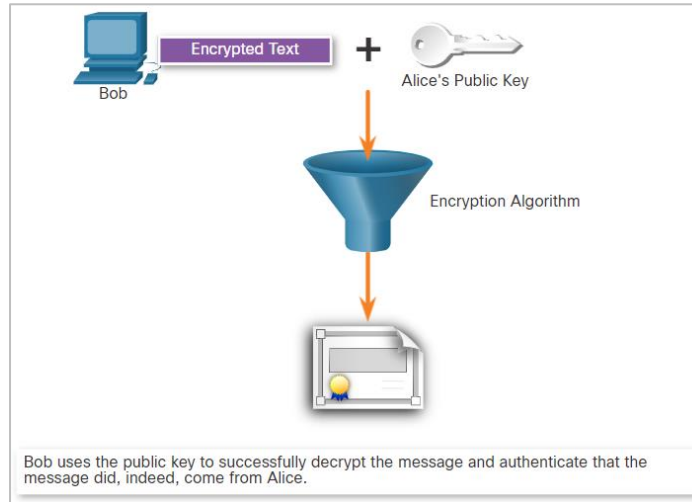
Alice uses her private key

Alice encrypts a message using her private key and sends it to Bob.



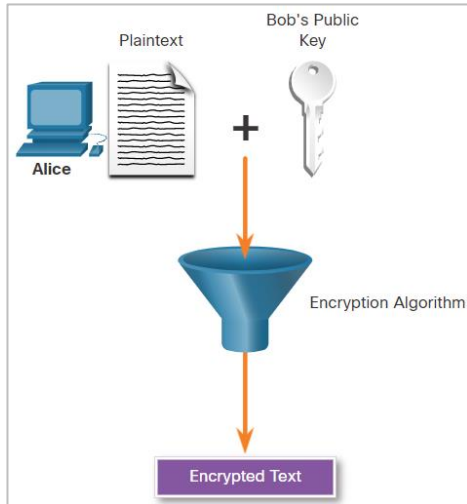
Bob decrypts using the public key

After Bob obtains Alice's public key, he uses it to decrypt the message and to authenticate that the message has been received from Alice.

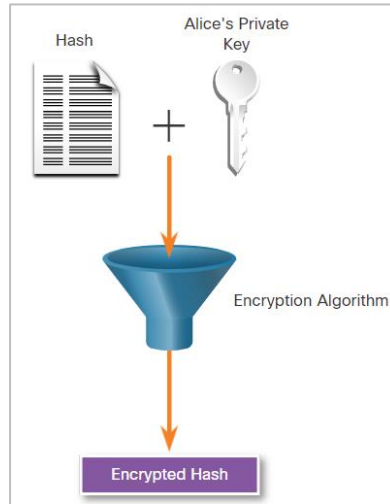


Asymmetric Encryption - Integrity

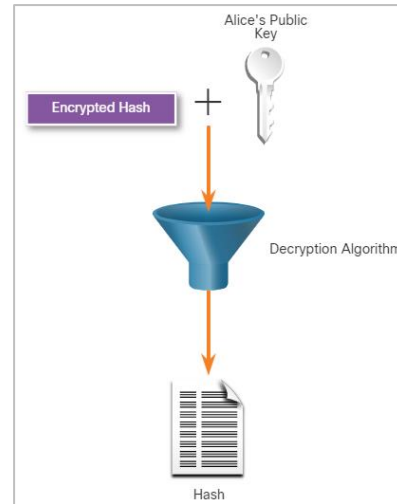
- Combining the two asymmetric encryption processes provides message confidentiality, authentication, and integrity. In this example, a message will be ciphered using Bob's public key and a ciphered hash will be encrypted using Alice's private key.



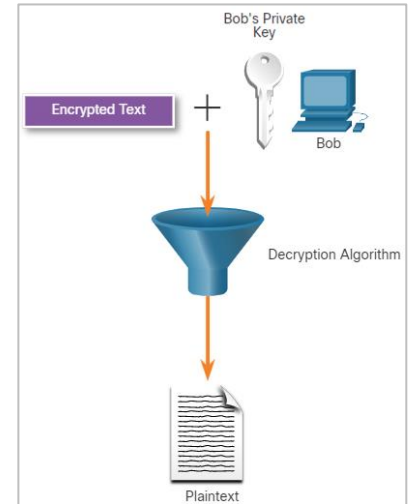
Alice uses Bob's
Public Key



Alice encrypts a
hash using her
private key



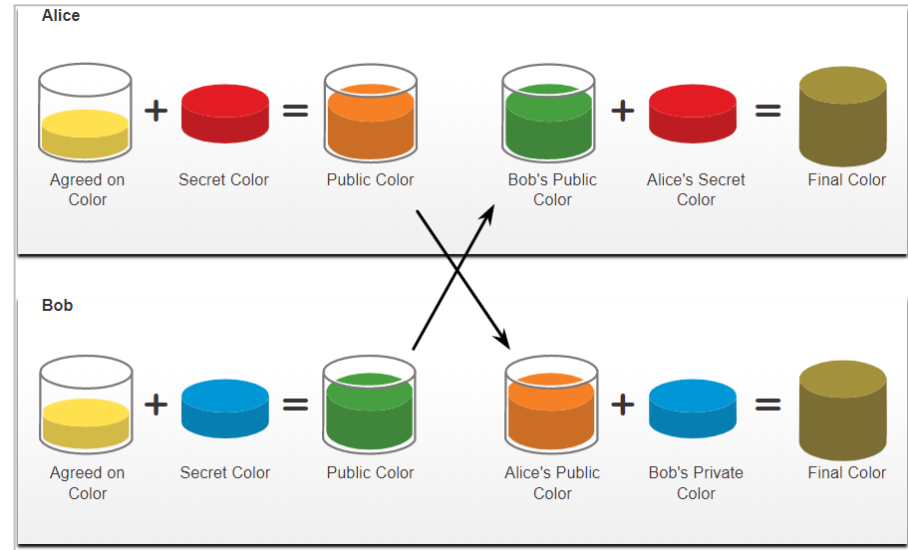
Bob uses Alice's
public key to
decrypt the hash



Bob uses his private
key to decrypt the
message

Diffie-Hellman

- Diffie-Hellman (DH) is an asymmetric mathematical algorithm that allows two computers to generate an identical shared secret without having communicated before.
- The new shared key is never actually exchanged between the sender and receiver.
- The key can be used by an encryption algorithm to encrypt traffic between the two systems as both parties know it.
- Following are two examples of instances when DH is commonly used:
 - Data is exchanged using an IPsec VPN
 - SSH data is exchanged
 - The security of DH is based on the fact that it uses very large numbers in its calculations.



DH operation

Diffie-Hellman (Contd.)

- Diffie-Hellman uses different DH groups to determine the strength of the key that is used in the key agreement process. The higher group numbers are more secure, but require additional time to compute the key.
- The following identifies the DH groups supported by Cisco IOS Software and their associated prime number value:
 - DH Group 1: 768 bits
 - DH Group 2: 1024 bits
 - DH Group 5: 1536 bits
 - DH Group 14: 2048 bits
 - DH Group 15: 3072 bits
 - DH Group 16: 4096 bits
- **Note:** *A DH key agreement can also be based on elliptic curve cryptography. DH groups 19, 20, and 24, are supported by Cisco IOS Software.*

Lab - Encrypting and Decrypting Data Using OpenSSL

- In this lab, you will complete the following objectives:
- Encrypting Messages with OpenSSL
- Decrypting Messages with OpenSSL

Lab - Encrypting and Decrypting Data Using a Hacker Tool

- In this lab, you will complete the following objectives:
- Setup Scenario
- Create and Encrypt Files
- Recover Encrypted Zip File Passwords

Lab - Examining Telnet and SSH in Wireshark

- In this lab, you will complete the following objectives:
- Examine a Telnet Session with Wireshark
- Examine an SSH Session with Wireshark

21.3 Public Key Cryptography

Using Digital Signatures

- Digital signatures are a mathematical technique used to provide authenticity, integrity, and nonrepudiation.
- Digital signatures use asymmetric cryptography.
- Digital signatures are commonly used in the following two situations:
 - Code signing - Code signing is used to verify the integrity of executable files downloaded from a vendor website. It also uses signed digital certificates to authenticate and verify the identity of the site that is the source of the files.
 - Digital certificates - These are used to authenticate the identity of a system with a vendor website and establish an encrypted connection to exchange confidential data.
- The Digital Signature Standard (DSS) algorithms used for generating and verifying digital signatures are:
 - **Digital Signature Algorithm (DSA)**
 - **Rivest-Shamir Adelman Algorithm (RSA)**
 - **Elliptic Curve Digital Signature Algorithm (ECDSA)**

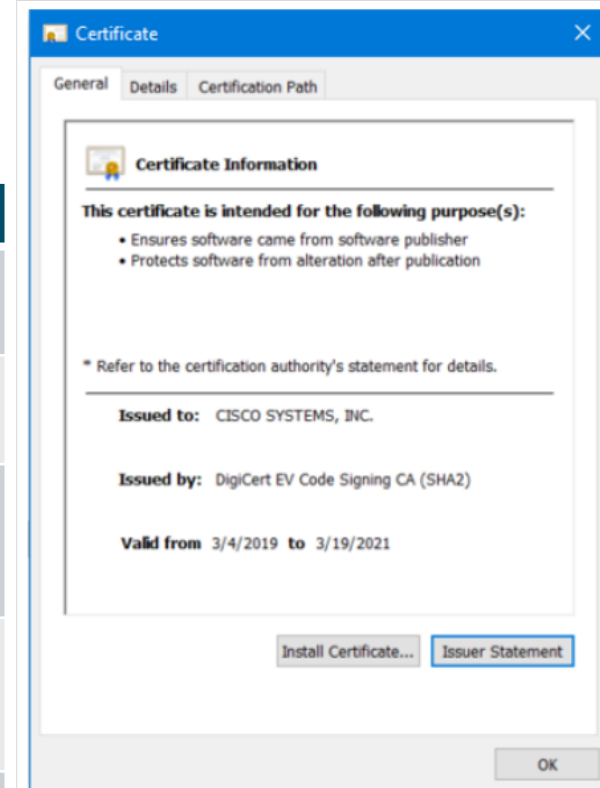
Digital Signatures for Code Signing

- Digital signatures are commonly used to provide assurance of the authenticity and integrity of software code.
- Executable files are wrapped in a digitally signed envelope, which allows the end user to verify the signature before installing the software.
- Digitally signing code provides several assurances about the code:
 - The code is authentic and is actually sourced by the publisher.
 - The code has not been modified since it left the software publisher.
 - The publisher undeniably published the code. This provides nonrepudiation of the act of publishing.
- The purpose of digitally signed software is to ensure that the software has not been tampered with, and that it originated from the trusted source as claimed.

Digital Signatures for Code Signing (Contd.)

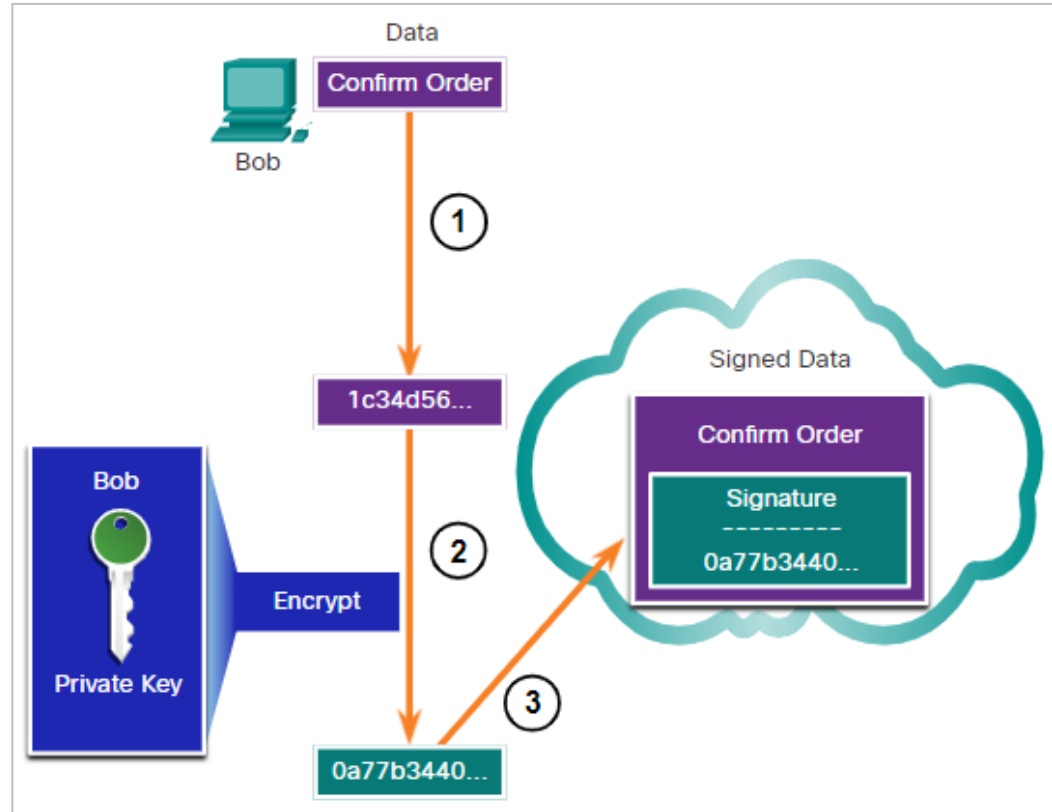
- The properties of a file that has a digitally signed certificate are as follows:

Properties	Description
File Properties	This executable file was downloaded from the internet and it contains a software tool from Cisco Systems.
Digital Signatures	This tab reveals that the file is from a trusted organization, Cisco Systems Inc.
Digital Signatures Details	This window reveals that the file was signed by Cisco Systems, Inc mentioning the given year, month and time.
Certificate Information	The General tab provides information such as who the certificate was issued to, and who issued the certificate. It also displays the period for which the certificate is valid.
Certificate Path	In this tab, you can see the file was signed by Cisco Systems, as verified to DigiCert.



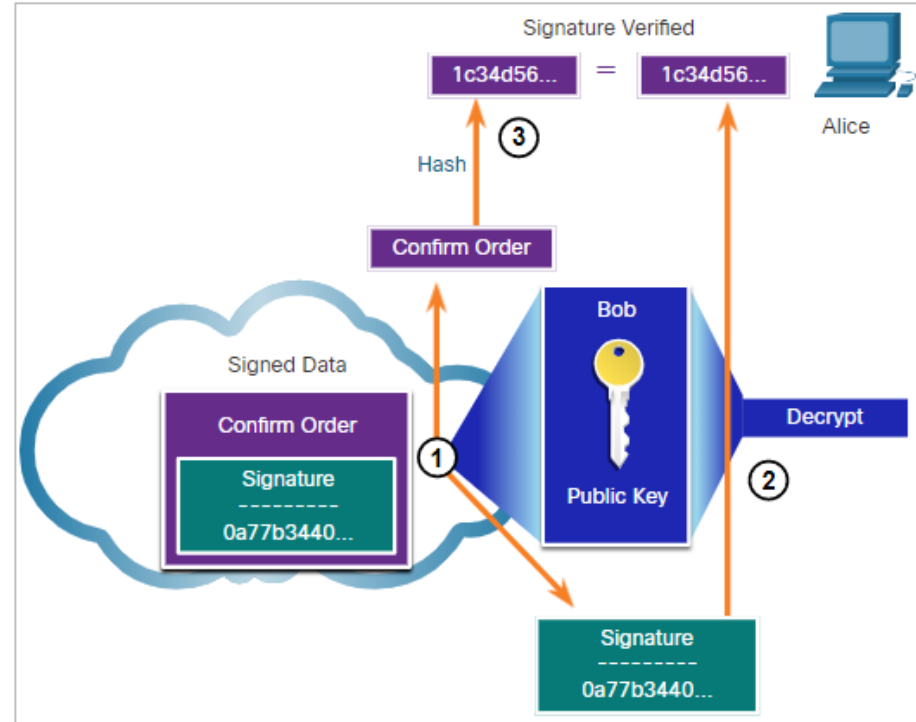
Digital Signatures for Digital Certificates (Contd.)

- This scenario will help you understand how a digital signature is used.
- Bob is confirming an order with Alice, which she is ordering from Bob's website.
- Bob confirms the order and his computer creates a hash of the confirmation.
- The computer encrypts the hash with Bob's private key.
- The encrypted hash, which is the digital signature, is added to the document.
- The order confirmation is then sent to Alice over the internet.



Digital Signatures for Digital Certificates (Contd.)

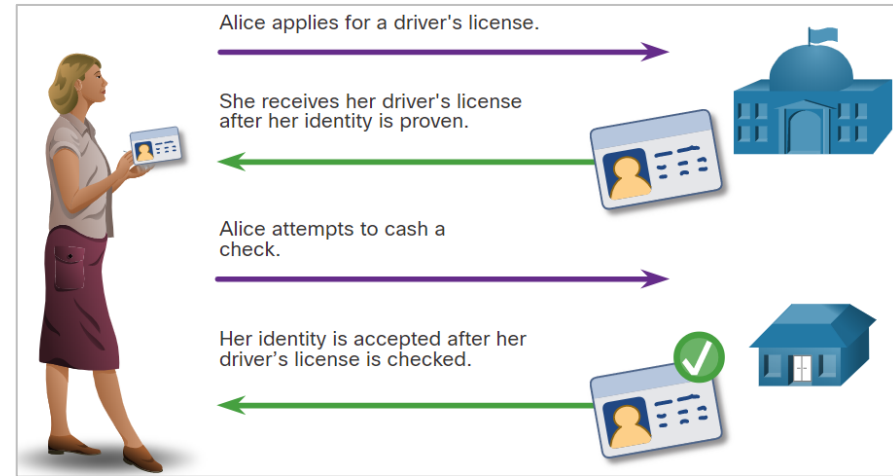
- When Alice receives the digital signature, the following process occurs:
- Alice's receiver accepts the order confirmation with the digital signature and obtains Bob's public key.
- Alice's computer then decrypts the signature using Bob's public key which reveals the assumed hash value of the sending device.
- Alice's computer creates a hash of the received document, without its signature, and compares this hash to the decrypted hash.
- If the hashes match, the document is authentic. This means the confirmation was sent by Bob and has not changed since signed.



21.4 Authorities and the PKI Trust System

Public Key Management

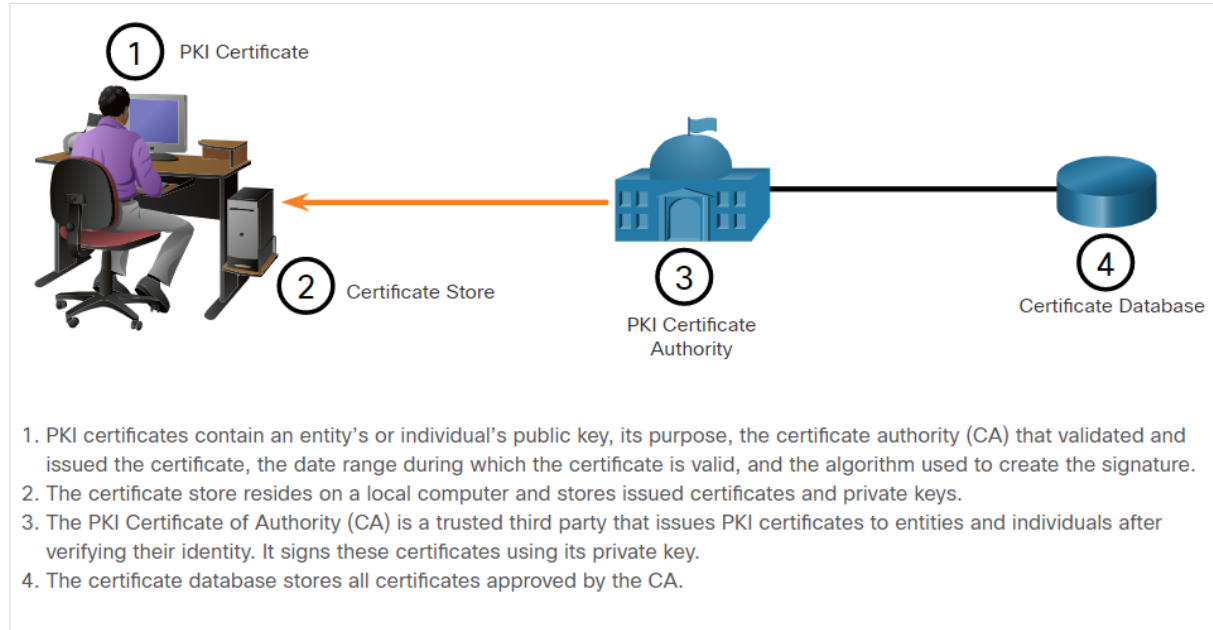
- When establishing an asymmetric connection between two hosts, the hosts will exchange their public key information.
- Trusted third parties on the Internet validate the authenticity of these public keys using digital certificates. The third-party issues credentials that are difficult to forge.
- From that point forward, all individuals who trust the third party simply accept the credentials that the third-party issues.
- The Public Key Infrastructure (PKI) consists of specifications, systems, and tools that are used to create, manage, distribute, use, store, and revoke digital certificates.
- The Certificate Authority (CA) creates digital certificates by tying a public key to a confirmed identify, such as a website or individual.



Illustrates how a driver's license is analogous to a digital certificate

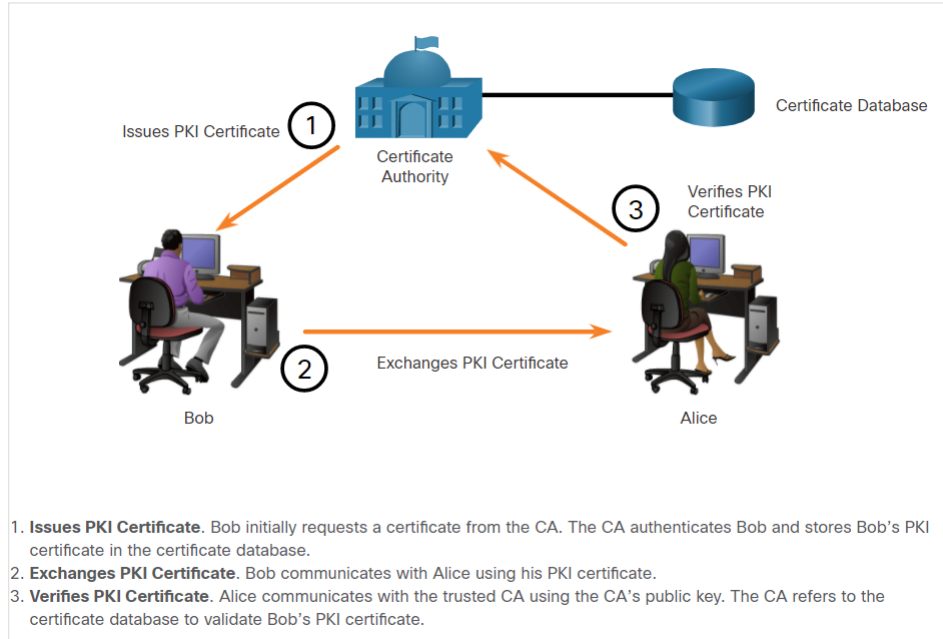
The Public Key Infrastructure

- PKI is needed to support large-scale distribution and identification of public encryption keys.
- The PKI framework facilitates a highly scalable trust relationship.
- It consists of the hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates.
- The figure shows the main elements of the PKI.



The Public Key Infrastructure (Contd.)

- The below figure shows how the elements of the PKI interoperate:



- **Note:** Not all PKI certificates are directly received from a CA. A Registration Authority (RA) is a subordinate CA and is certified by a root CA to issue certificates for specific uses.

The PKI Authorities System

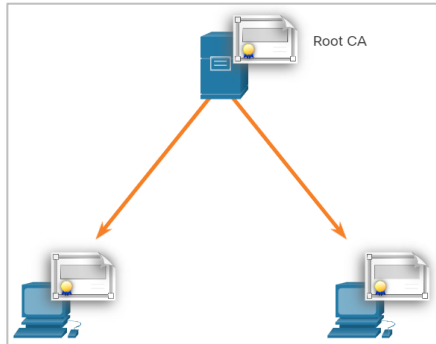
- Many vendors provide CA servers as a managed service or as an end-user product.
- Organizations may also implement private PKIs using Microsoft Server or Open SSL.
- CAs issue certificates based on classes which determine how trusted a certificate is.
- The class number is determined by how rigorous the procedure was that verified the identity of the holder when the certificate was issued.
- The higher the class number, the more trusted the certificate.
- Some CA public keys are preloaded, such as those listed in web browsers.

Class	Description
0	Used for testing in situations in which no checks have been performed.
1	Used by individuals who require verification of email.
2	Used by organizations for which proof of identity is required.
3	Used for servers and software signing.
4	Used for online business transactions between companies.
5	Used for private organizations or government security.

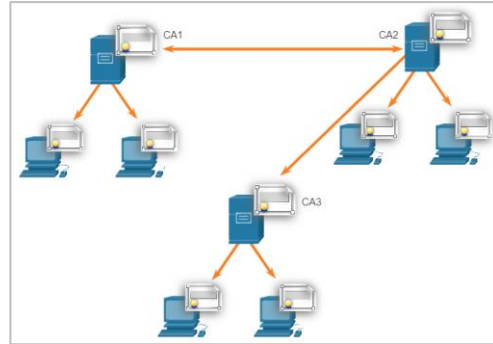
Note: An enterprise can also implement PKI for internal use. PKI can be used to authenticate employees who are accessing the network. In this case, the enterprise is its own CA.

The PKI Trust System

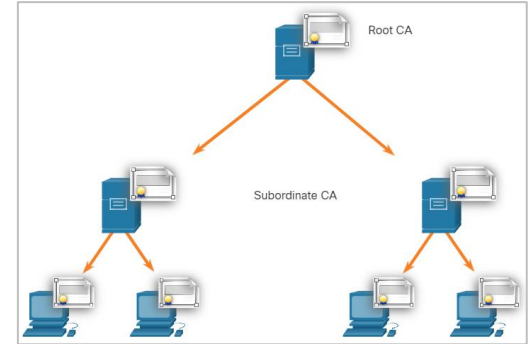
- PKIs can form different topologies of trust which are as follows:
 - Single-Root PKI Topology:** The simplest is the single-root PKI topology. The root CA issues all the certificates to the end users within the same organization. On larger networks, PKI CAs may be linked using two basic architectures:
 - Cross-certified CA topologies:** A peer-to-peer model in which individual CAs establish trust relationships with other CAs by cross-certifying CA certificates.
 - Hierarchical CA topologies:** The root CA (highest level CA), can issue certificates to end users and to a subordinate CA.



Single-Root PKI
Topology



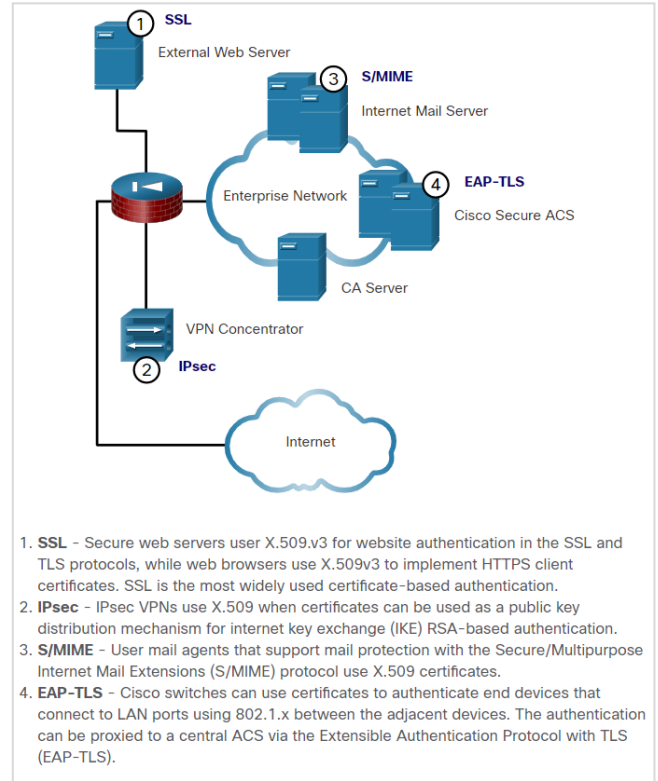
Cross-certified CA
Topologies



Hierarchical CA Topologies

Interoperability of Different PKI Vendors

- Interoperability between a PKI and its supporting services is a concern because many CA vendors have proposed and implemented proprietary solutions.
- To address this interoperability concern, the IETF published the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527).
- The X.509 version 3 (X.509 v3) standard defines the format of a digital certificate.
- **Note:** *LDAP and X.500 are protocols that are used to query a directory service, such as Microsoft Active Directory, to verify a username and password.*



X.509v3 Applications

Certificate Enrollment, Authentication and Revocation

- All systems that leverage the PKI must have the CA's public key, which is called the self-signed certificate.
- The CA public key verifies all the certificates issued by the CA and is vital for the proper operation of the PKI.
- The certificate enrollment process is used by a host system to enroll with a PKI. To do so, CA certificates are retrieved in-band over a network, and the authentication is done out-of-band (OOB) using the telephone.
- The system enrolling with the PKI contacts a CA to request and obtain a digital identity certificate for itself and to get the CA's self-signed certificate.
- The final stage verifies that the CA certificate was authentic and is performed using an out-of-band method such as the POTS to obtain the fingerprint of the valid CA identity certificate.
- A digital certificate can be revoked if key is compromised or if it is no longer needed.
- **Note:** *Only a root CA can issue a self-signed certificate that is recognized or verified by other CAs within the PKI.*

Lab – Certificate Authority Stores

- In this lab, you will complete the following objectives:
- Certificates Trusted by Your Browser
- Checking for Man-In-Middle

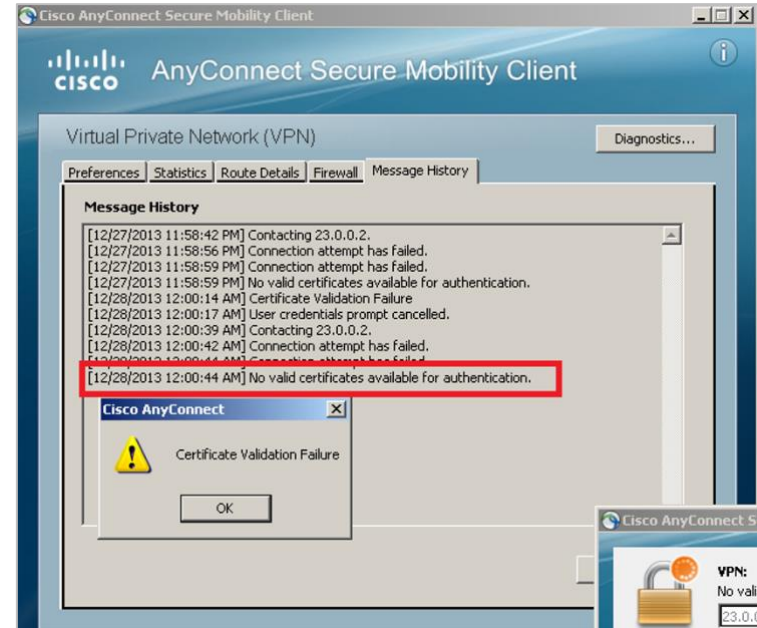
21.5 Applications and Impacts of Cryptography

PKI Applications

- The following provides a short list of common uses of PKIs:
- SSL/TLS certificate-based peer authentication
- Secure network traffic using IPsec VPNs
- HTTPS Web traffic
- Control access to the network using 802.1x authentication
- Secure email using the S/MIME protocol
- Secure instant messaging
- Approve and authorize applications with Code Signing
- Protect user data with the Encryption File System (EFS)
- Implement two-factor authentication with smart cards
- Securing USB storage devices

Encrypted Network Transactions

- Threat actors can use SSL/TLS to introduce regulatory compliance violations, viruses, malware, data loss, and intrusion attempts in a network.
- Other SSL/TLS-related issues may be associated with validating the certificate of a web server. When this occurs, the web browsers will display a security warning. PKI-related issues associated with security warnings include:
 - Validity date range - The X.509v3 certificates specify “not before” and “not after” dates. If the current date is outside the range, the web browser displays a message.
- **Signature validation error** - If a browser cannot validate the signature on the certificate, there is no assurance that the public key in the certificate is authentic.



Encryption and Security Monitoring

- Network monitoring becomes more challenging when packets are encrypted.
- As HTTPS introduces end-to-end encrypted HTTP traffic (via TLS/SSL), it is not as easy to peek into user traffic.
- Security analysts must know how to circumvent and solve these issues. Here is a list of some of the things that a security analyst could do:
 - Configure rules to distinguish between SSL and non-SSL traffic, HTTPS and non-HTTPS SSL traffic.
 - Enhance security through server certificate validation using CRLs and OCSP.
 - Implement antimalware protection and URL filtering of HTTPS content.
 - Deploy a Cisco SSL Appliance to decrypt SSL traffic and send it to intrusion prevention system (IPS) appliances to identify risks normally hidden by SSL.

Encryption and Security Monitoring (Contd.)

- Cryptography is dynamic and always changing. A security analyst must maintain a good understanding of cryptographic algorithms and operations to be able to investigate cryptography-related security incidents.
- There are two main ways in which cryptography impacts security investigations.
- First, attacks can be directed to specifically target the encryption algorithms themselves.
- After the algorithm has been cracked and the attacker has obtained the keys, any encrypted data that has been captured can be decrypted by the attacker and read, thus exposing private data.
- Secondly, the security investigation is also affected because data can be hidden in plain sight by encrypting it.

21.6 Public Key Cryptography Summary

What Did I Learn in this Module?

- The four elements of secure communications: data integrity, origin authentication, data confidentiality, and data non-repudiation.
- A hash function takes a variable block of binary data, called the message, and produces a fixed-length, condensed representation, called the hash.
- There are two classes of encryption that are used to provide data confidentiality: asymmetric and symmetric.
- Symmetric encryption algorithms, such as DES, 3 DES, and AES are based on the premise that each communicating party knows the pre-shared key.
- Asymmetric algorithms (public key algorithms) are designed so that the key that is used for encryption is different from the key used for decryption.
- Data confidentiality can also be ensured using asymmetric algorithms, including Rivest, Shamir, and Adleman (RSA) and PKI. The process is summarized using this formula: Public key (Encrypt) + Private Key (Decrypt) = Confidentiality.

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

- The authentication objective of an asymmetric algorithm is initiated when the encryption process is started with the private key. The process can be summarized with this formula: Private Key (Encrypt) + Public Key (Decrypt) = Authentication.
- Diffie-Hellman (DH) is an asymmetric mathematical equation algorithm that allows two computers to generate an identical shared secret key without having communicate before.
- Digital signatures are a mathematical technique used to provide three basic security services: authenticity, integrity, and non-repudiation. Digital signatures are commonly used in code signing and digital certificates.
- The Public Key Infrastructure (PKI) consists of specifications, systems, and tools that are used to create, manage, distribute, use, store, and revoke digital certificates.
- There are many common uses of PKIs including a few listed here: SSL/TLS certificate-based peer authentication, HTTPS Web traffic, secure instant message, and securing USB storage devices.
- A security analyst must be able to recognize and solve potential problems related to permitting PHI-related solutions on the enterprise network.

Thank you! Questions?



Vladimír Veselý

updated: 2023-03-27

<https://www.fit.vutbr.cz/research/groups/nes@fit>

Module 22: Endpoint Protection

Instructor Materials

CyberOps Associate v1.0

Module 22: Endpoint Protection

CyberOps Associate v1.0

Module Objectives

Module Title: Endpoint Protection

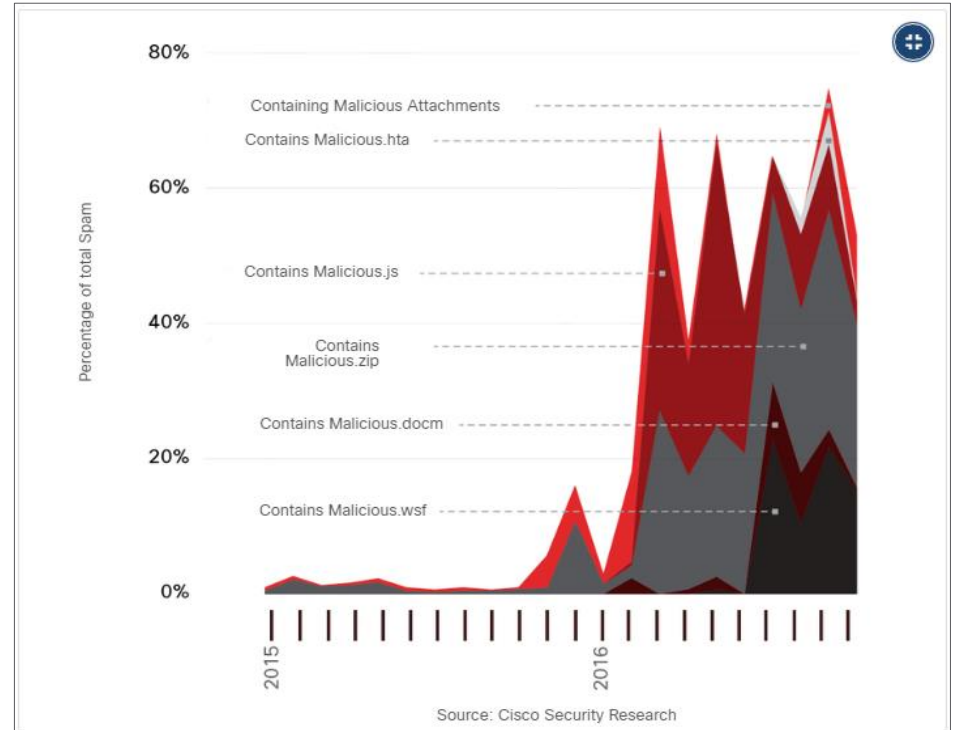
Module Objective: Explain how a malware analysis website generates a malware analysis report.

Topic	Topic Objective
Antimalware Protection	Explain methods of mitigating malware
Host-based Intrusion Prevention	Explain host-based IPS/IDS log entries
Application Security	Explain how a sandbox is used to analyze malware

22.1 Antimalware Protection

Endpoint Threats

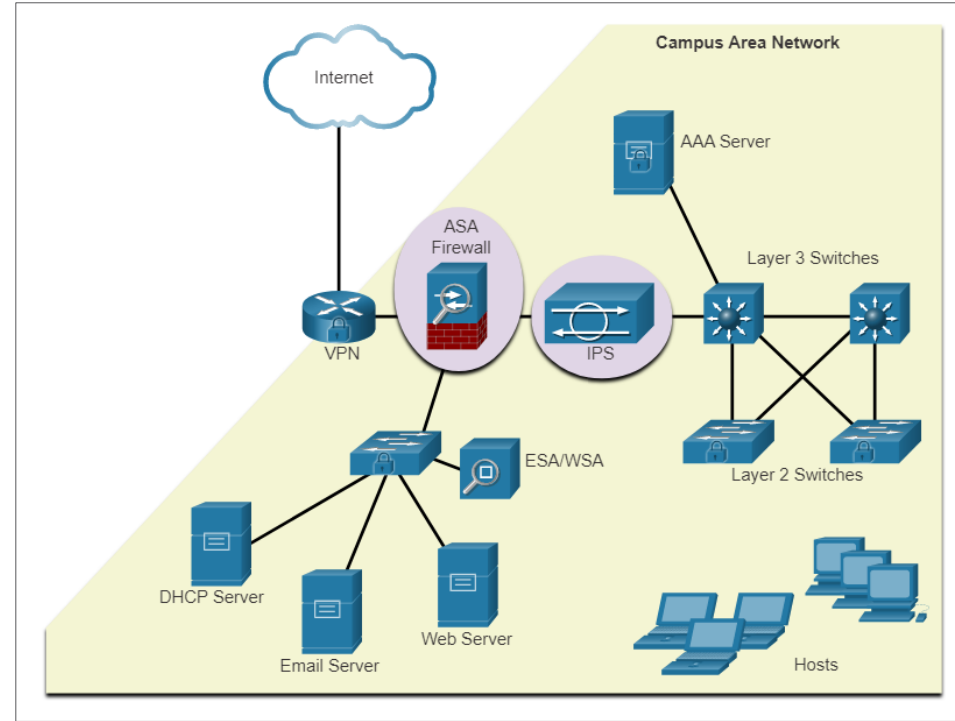
- Endpoints can be defined as hosts on the network that can access or be accessed by other hosts on the network.
- Each endpoint is potentially a way for malicious software to gain access to a network.
- Devices that remotely access networks through VPNs are also endpoints that could inject malware into the VPN network from the public network.
- Several common types of malware have been found to significantly change features in less than 24 hours in order to evade detection.



Malicious Spam Percentage

Endpoint Security

- As many attacks originate from inside the network, securing an internal LAN is nearly as important as securing the outside network perimeter.
- After an internal host is infiltrated, it can become a starting point for an attacker to gain access to critical system devices, such as servers and sensitive information.
- There are two internal LAN elements to secure:
- Endpoints - Hosts are susceptible to malware-related attacks.
- Network infrastructure - LAN infrastructure devices interconnect endpoints

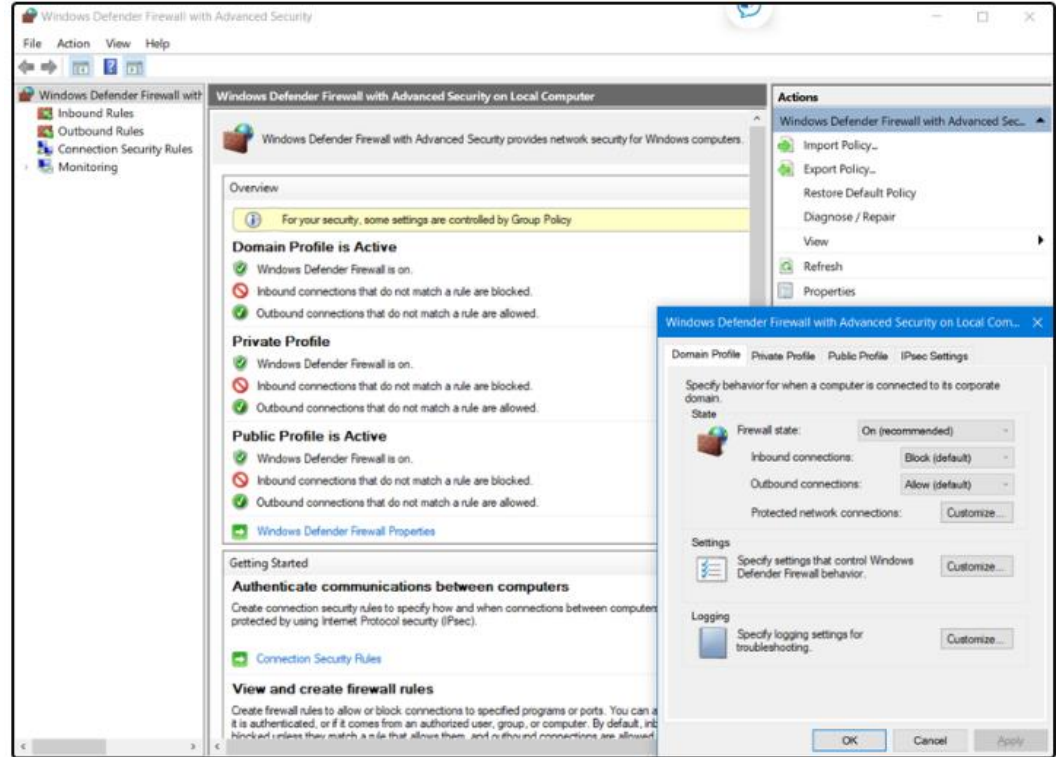


Host-Based Malware Protection

- Host-based antimalware/antivirus software and host-based firewalls are used to protect mobile devices using VPN.
- Antivirus/Antimalware Software
- It is a software that is installed on a host to detect and mitigate viruses and malware. For example, Windows Defender Virus & Threat Protection, Cisco AMP for Endpoints, Norton Security, McAfee, Trend Micro, and others.
- Antimalware programs may detect viruses using three different approaches:
 - **Signature-based:** Recognizes various characteristics of known malware files
 - **Heuristics-based:** Recognizes general features shared by various types of malware
 - **Behavior-based:** Employs analysis of suspicious behavior
- Host-based antivirus protection, also known as agent-based, runs on every protected machine.

Host-Based Malware Protection (Contd.)

- Host-based Firewall
- This software is installed on a host.
- It restricts incoming and outgoing connections to connections initiated by that host only.
- Some firewall software can prevent a host from becoming infected and stop infected hosts from spreading malware to other hosts. This function is included in some operating systems.
- For example, Windows includes Windows Defender Firewall with Advanced Security.

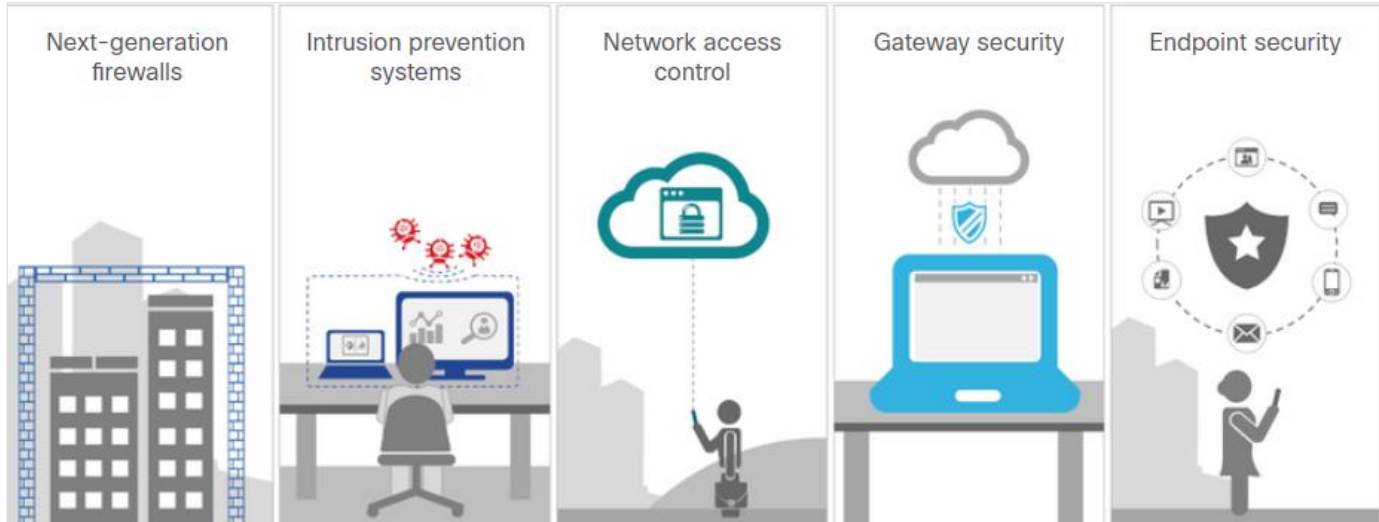


Host-Based Malware Protection (Contd.)

- Host-based Security Suites
- It is recommended to install a host-based suite of security products on home and business networks to provide a layered defense that will protect against most common threats.
- These include antivirus, anti-phishing, safe browsing, Host-based intrusion prevention system, and firewall capabilities.
- Host-based security products also provide telemetry function.
- Most host-based security software includes robust logging functionality that is essential to cyber security operations.
- The independent testing laboratory AV-TEST provides high-quality reviews of host-based protections, as well as information about many other security products.

Network-Based Malware Protection

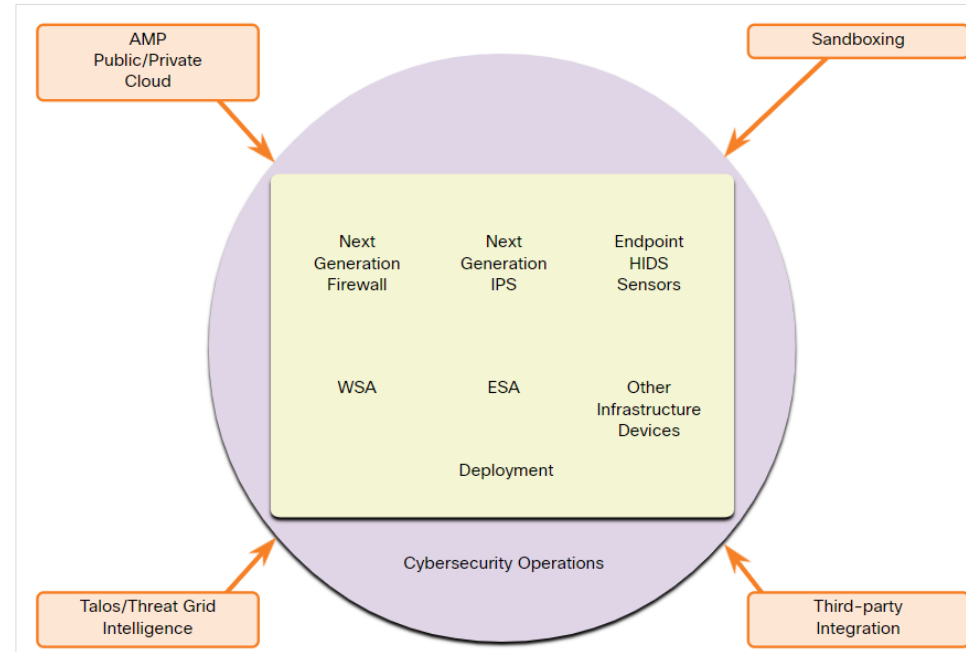
- Network-based malware prevention devices are capable of sharing information among themselves to make better informed decisions.
- Protecting endpoints in a borderless network can be accomplished using network-based, as well as host-based techniques.



Advanced Malware Protection Everywhere

Network-Based Malware Protection (Contd.)

- Some examples of devices and techniques that implement host protections at the network level:
 - Advanced Malware Protection (AMP) - Provides endpoint protection from viruses and malware.
 - Email Security Appliance (ESA) - Provides filtering of SPAM and potentially malicious emails before they reach the endpoint.
 - Web Security Appliance (WSA) - Provides filtering of websites and blacklisting
 - Network Admission Control (NAC) - Permits only authorized and compliant systems to connect to the network.



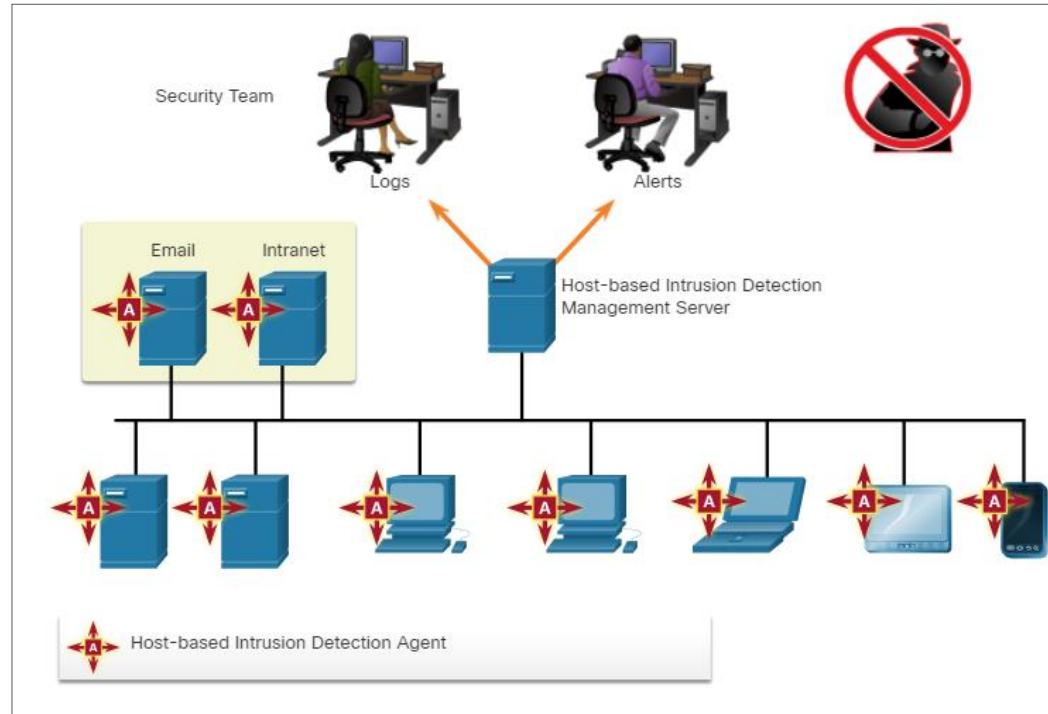
22.2 Host-Based Intrusion Protection

Host-Based Firewalls

- Host-based personal firewalls are standalone software programs that control traffic entering or leaving a computer.
- Host-based firewall applications can also be configured to issue alerts to users if suspicious behavior is detected.
- Some examples of host-based firewalls:
 - Windows Defender Firewall – First included with Windows XP, Windows Firewall (now Windows Defender Firewall) uses a profile-based approach to firewall functionality.
 - iptables – This is an application that allows Linux system administrators to configure network access rules that are part of the Linux kernel Netfilter modules.
 - nftables – The successor to iptables, nftables is a Linux firewall application that uses a simple virtual machine in the Linux kernel.
 - TCP Wrappers – This is a rule-based access control and logging system for Linux.

Host-Based Intrusion Detection

- A Host-based Intrusion Detection System (HIDS) is designed to protect hosts against known and unknown malware.
- A HIDS can perform detailed monitoring and reporting on the system configuration and application activity.
- HIDS is a comprehensive security application that combines the functionalities of antimalware applications with firewall functionality.
- As HIDS must run directly on the host, it is considered as an agent-based system.



Host-based Intrusion Detection Architecture

HIDS Operation

- A HIDS can prevent intrusion because it uses signatures to detect known malware and prevent it from infecting a system.
- Some malware families exhibit polymorphism.
- An additional set of strategies are used to detect the possibility of successful intrusions by malware that evades signature detection:
 - Anomaly based - Host system behavior is compared to a learned baseline model of normal behavior. If an intrusion is detected, the HIDS can log details of the intrusion, send alerts to security management systems, and take action to prevent the attack.
 - Policy based - Normal system behavior is described by rules, or the violation of rules, that are predefined. Violation of these policies will result in action by the HIDS, such as shut down of software processes.

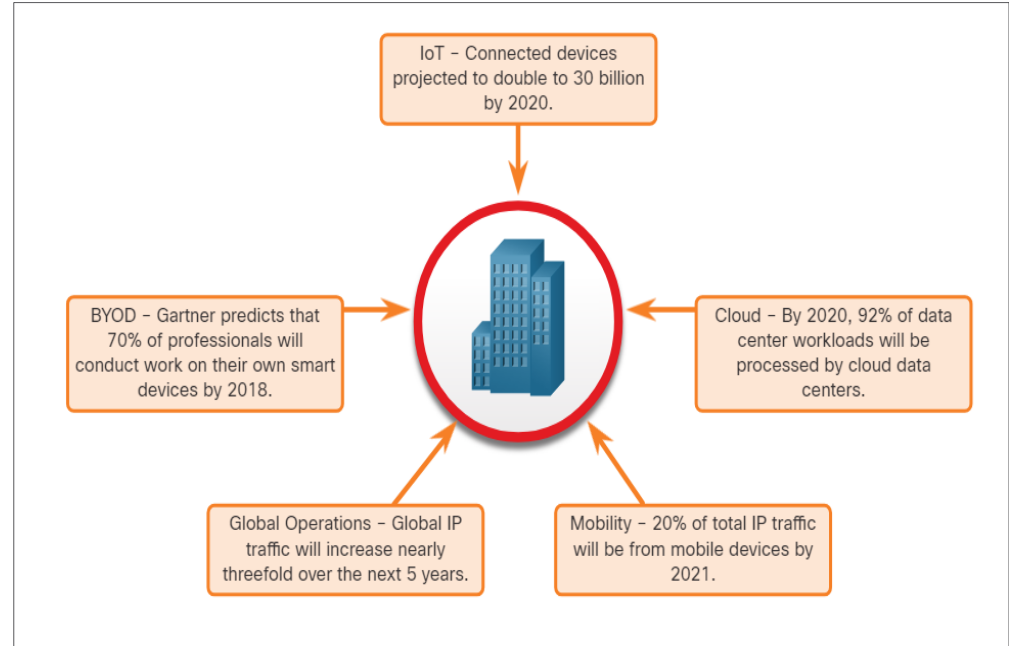
HIDS Products

- Most of the HIDS utilize software on the host and some sort of centralized security management functionality that allows integration with network security monitoring services and threat intelligence.
- Some examples are Cisco AMP, AlienVault USM, Tripwire, and Open Source HIDS SECURITY (OSSEC).
- OSSEC uses a central manager server and agents that are installed on individual hosts.
- The OSSEC server, or Manager, can also receive and analyze alerts from a variety of network devices and firewalls over syslog.
- OSSEC monitors system logs on hosts and also conducts file integrity checking.

22.3 Application Security

Attack Surface

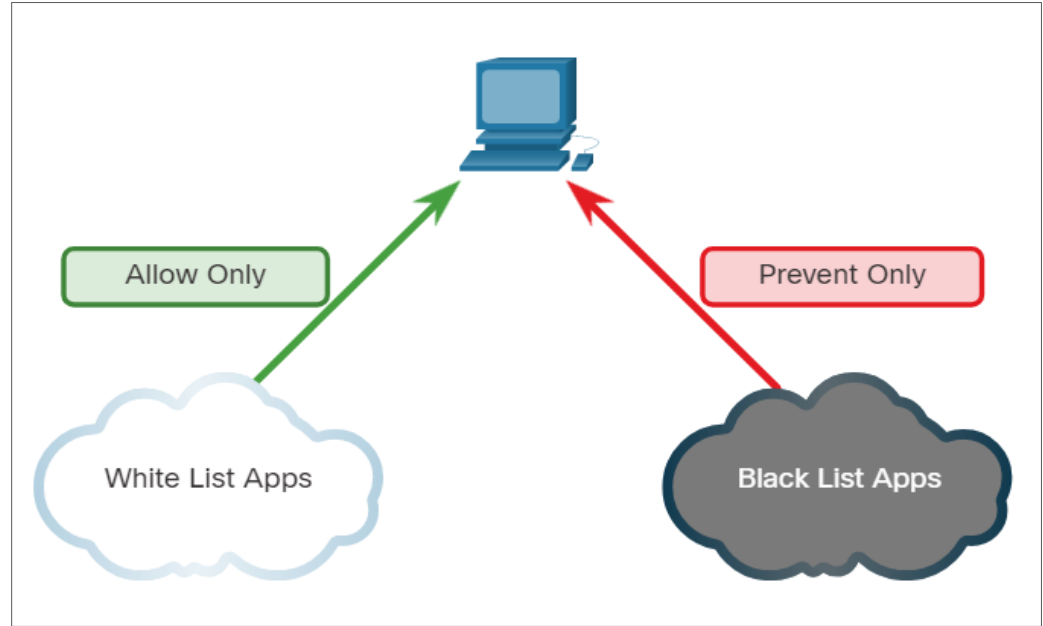
- An attack surface is the total sum of the vulnerabilities in a given system that is accessible to an attacker.
- It can consist of open ports on servers or hosts, software running on internet-facing servers, wireless network protocols, and users.
- Components of the Attack Surface:
 - **Network Attack Surface:** Exploits vulnerabilities in networks.
 - **Software Attack Surface:** Delivered through exploitation of vulnerabilities in web, cloud, or host-based software applications.
 - **Human Attack Surface:** Exploits weaknesses in user behavior.



An Expanding Attack Surface

Application Blacklisting and Whitelisting

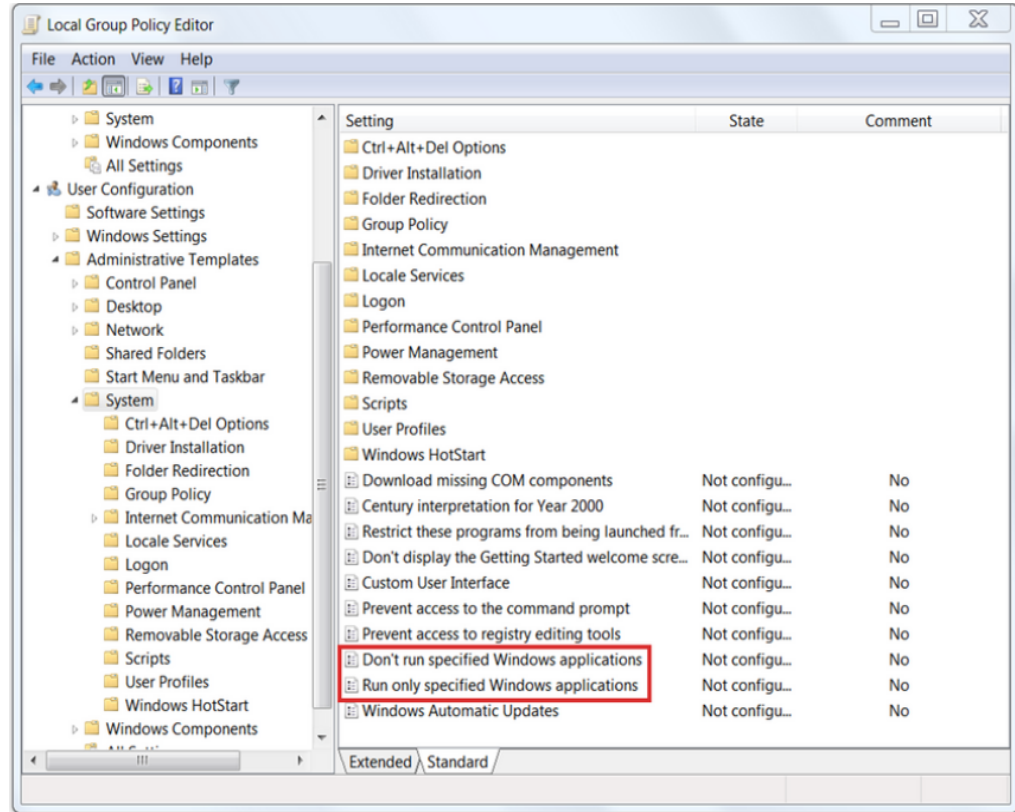
- Limiting access to potential threats by creating lists of prohibited applications is known as blacklisting.
- Application blacklists can dictate which user applications are not permitted to run on a computer.
- Whitelists specify which programs are allowed to run.
- In this way, known vulnerable applications can be prevented from creating vulnerabilities on network hosts.



Application Blacklisting and Whitelisting

Application Blacklisting and Whitelisting (Contd.)

- Websites can also be whitelisted and blacklisted.
- These blacklists can be manually created, or they can be obtained from various security services.
- Blacklists can be continuously updated by security services and distributed to firewalls and other security systems that use them.
- Cisco's Firepower security management system is an example of a system that can access the Cisco Talos security intelligence service to obtain blacklists.



System-Based Sandboxing

- Sandboxing is a technique that allows suspicious files to be executed and analyzed in a safe environment.
- Cuckoo Sandbox is a popular free malware analysis system sandbox. It can be run locally and have malware samples submitted to it for analysis.
- ANY.RUN is an online tool that offers the ability to upload a malware sample for analysis like any online sandbox.



22.4 Endpoint Protection Summary

What Did I Learn in this Module?

- Endpoints are defined as hosts on the network that can access or be accessed by other hosts on the network.
- There are two internal LAN elements to secure: Endpoints and Network Infrastructure.
- Antivirus/Antimalware Software is installed on a host to detect and mitigate viruses and malware.
- Host-based firewalls may use a set of predefined policies, or profiles, to control packets entering and leaving a computer.
- Some examples of host-based firewalls include Windows Defender Firewall, iptables, nftables, and TCP Wrappers.
- HIDS protects hosts against known and unknown malware.
- An attack surface is the total sum of the vulnerabilities in a given system that is accessible to an attacker.
- Application blacklists dictate which user applications are not permitted to run on a computer and whitelists specify which programs are allowed to run.

Module 22

New Terms and Commands

- Antivirus/Antimalware
- Endpoint

- Host-based firewall
- Sandboxing

- Host-based Intrusion Detection System (HIDS)
- Attack Surface

Thank you! Questions?



Vladimír Veselý

updated: 2023-03-27

<https://www.fit.vutbr.cz/research/groups/nes@fit>

Module 23: Endpoint Vulnerability Assessment

Instructor Materials

CyberOps Associate v1.0

Module 23: Endpoint Vulnerability Assessment

Module Objectives

Module Title: Endpoint Vulnerability Assessment

Module Objective: Explain how endpoint vulnerabilities are assessed and managed.

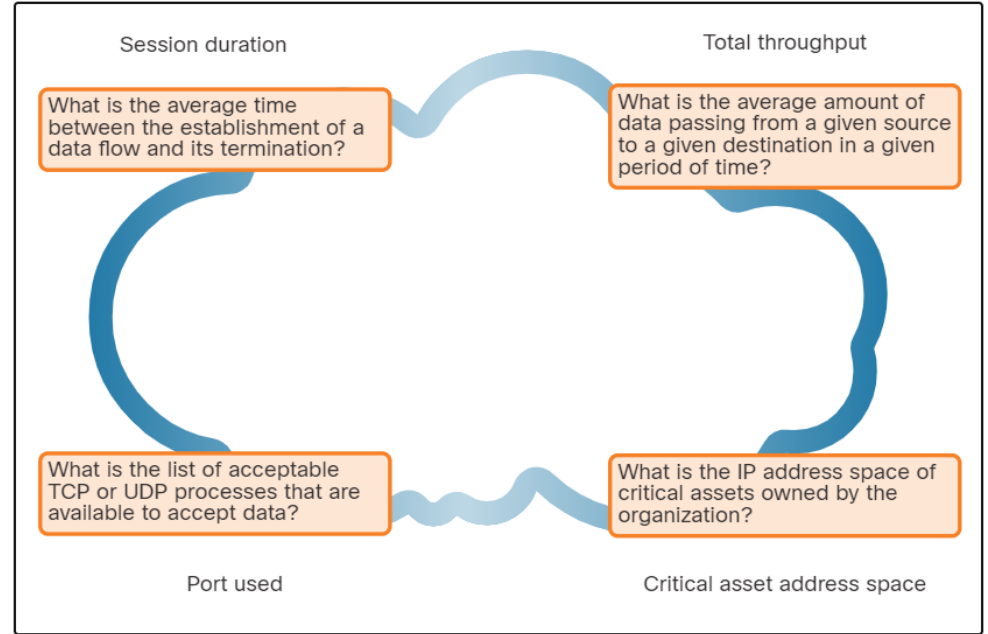
Content

Topic Title	Topic Objective
Network and Server Profiling	Explain the value of network and server profiling.
Common Vulnerability Scoring System (CVSS)	Explain how CVSS reports are used to describe security vulnerabilities.
Secure Device Management	Explain how secure device management techniques are used to protect data and assets.
Information Security Management Systems	Explain how information security management systems are used to protect assets.

23.1 Network and Server Profiling

Network Profiling

- Network and device profiling provides statistical baseline information that can serve as a reference point for normal network and device performance.
- Elements of network profile:
 - Session duration
 - Total throughput
 - Critical asset address space
 - Typical traffic type



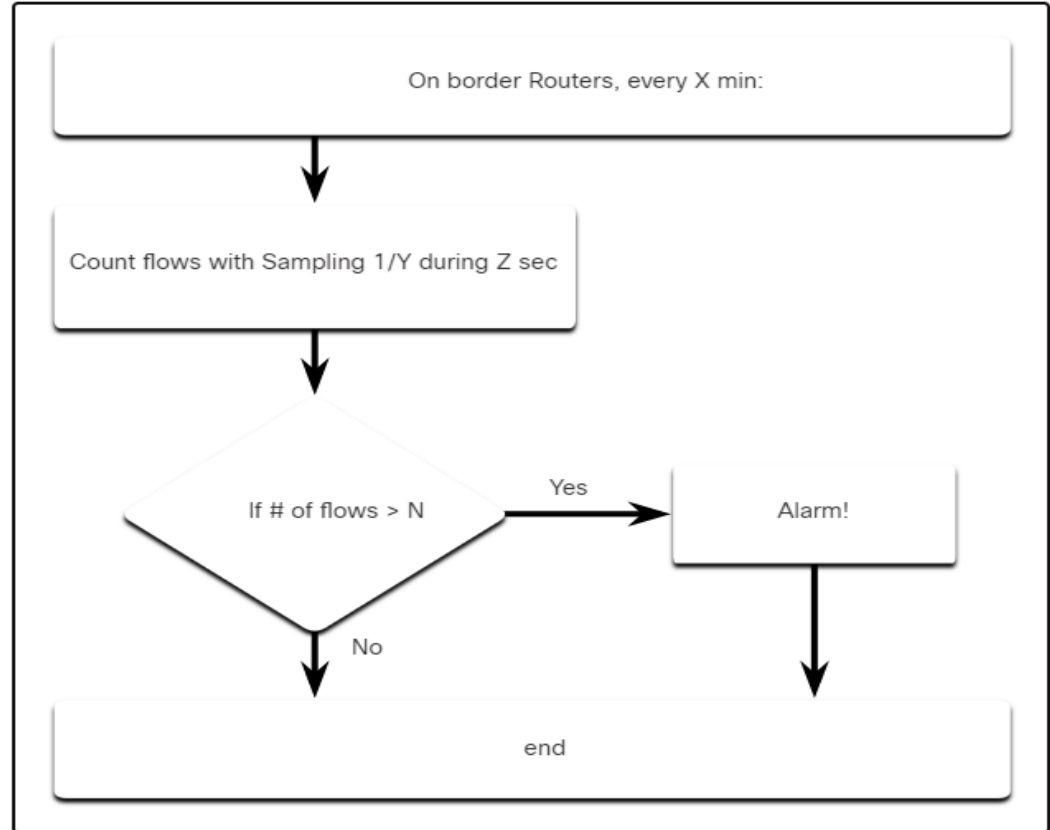
Elements of a Network Profile

Server Profiling

- A server profile is a security baseline for a given server.
- Server profiling is used to establish the accepted operating state of servers.
- The server profile elements are as follows:
 - Listening ports
 - Logged in users and accounts
 - Service accounts
 - Software environment

Network Anomaly Detection

- Network behavior is described by a large amount of diverse data such as the features of packet flow, features of the packets themselves, and telemetry from multiple sources.
- Big Data analytics techniques can be used to analyze this data and detect variations from the baseline.
- Anomaly detection can identify infected hosts on the network that are scanning for other vulnerable hosts.
- The figure illustrates a simplified version of an algorithm designed to detect an unusual condition at the border routers of an enterprise.



Network Vulnerability Testing

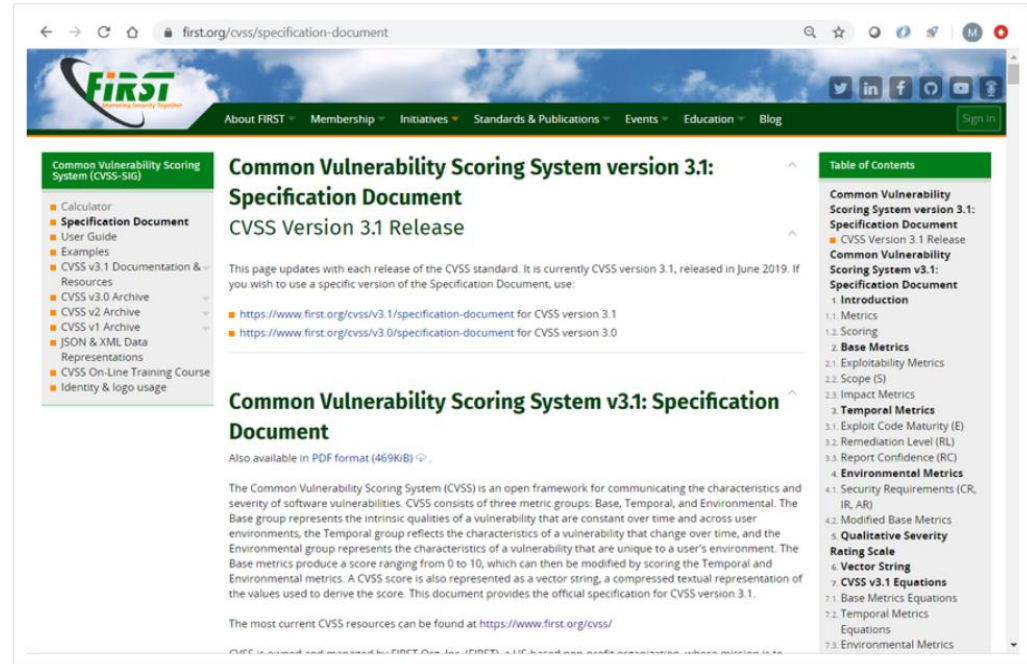
- Network Vulnerability Testing includes Risk Analysis, Vulnerability Assessment and Penetration Testing.

Activity	Description	Tools
Risk analysis	Individuals conduct comprehensive analysis of impacts of attacks on core company assets and functioning	Internal or external consultants, risk management frameworks
Vulnerability Assessment	Patch management, host scans, port scanning, other vulnerability scans and services	OpenVas, Microsoft Baseline Analyzer, Nessus, Qualys, Nmap
Penetration Testing	Use of hacking techniques and tools to penetrate network defenses and identify depth of potential penetration	Metasploit, CORE Impact, ethical hackers

23.2 Common Vulnerability Scoring System (CVSS)

CVSS Overview

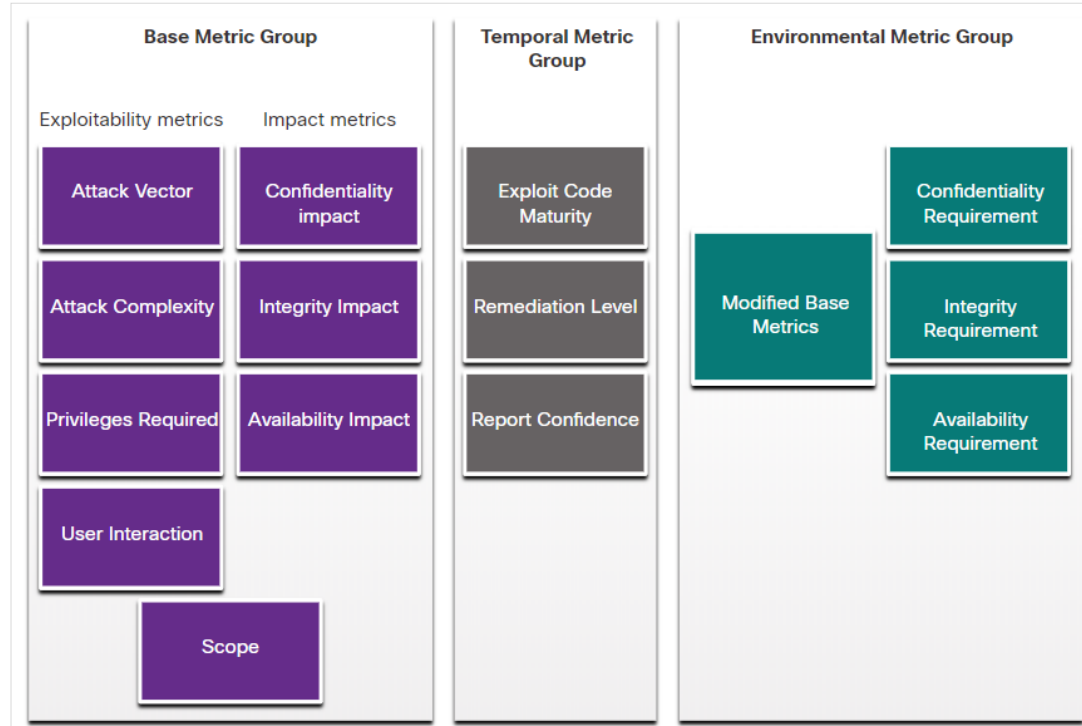
- The Common Vulnerability Scoring System (CVSS) is a risk assessment tool designed to convey the common attributes and severity of vulnerabilities in computer hardware and software systems.
- CVSS provides standardized vulnerability scores.
- It provides an open provides an open framework with metrics to all users.
- CVSS helps prioritize risk.
- The Forum of Incident Response and Security Teams (FIRST) has been designated as the custodian of the CVSS to promote its adoption globally.



The screenshot shows the web page for the CVSS 3.1 Specification Document. The browser address bar shows the URL first.org/cvss/specification-document. The page features a green header with the FIRST logo and navigation links: About FIRST, Membership, Initiatives, Standards & Publications, Events, Education, and Blog. A 'Sign in' button is located in the top right corner. The main content area is titled 'Common Vulnerability Scoring System version 3.1: Specification Document' and 'CVSS Version 3.1 Release'. Below the title, there is a paragraph stating that the page updates with each release of the CVSS standard, currently version 3.1, released in June 2019. Two links are provided for specific versions: <https://www.first.org/cvss/v3.1/specification-document> for CVSS version 3.1, and <https://www.first.org/cvss/v3.0/specification-document> for CVSS version 3.0. A 'Table of Contents' sidebar is visible on the right, listing sections such as Introduction, Metrics, Scoring, Base Metrics, Temporal Metrics, Environmental Metrics, and Security Requirements. A left sidebar contains a 'Common Vulnerability Scoring System (CVSS-310)' menu with items like Calculator, Specification Document, User Guide, Examples, and various archives.

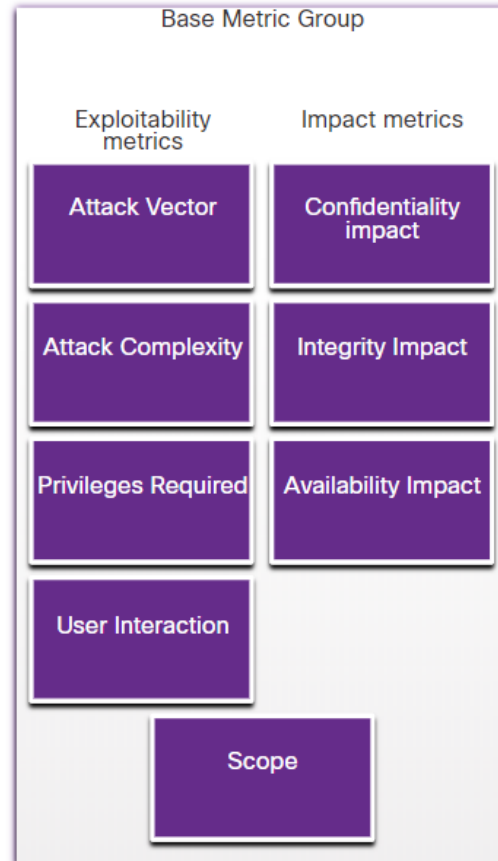
CVSS Metric Groups

- The CVSS uses three groups of metrics to assess vulnerability.
 - Base Metric Group: Represents the characteristics of a vulnerability that are constant over time and across contexts.
 - Temporal Metric Group: Measures the characteristics of a vulnerability that may change over time, but not across user environments.
 - Environmental Metric Group: Measures the aspects of a vulnerability that are rooted in a specific organization's environment.



CVSS Base Metric Group

- Base Metric Group Exploitability metrics include the following criteria:
 - Attack vector
 - Attack complexity
 - Privileges required
 - User interaction
 - Scope
- Base Metric Group Impact metrics components include the following criteria:
 - Confidentiality Impact
 - Integrity Impact
 - Availability Impact



The CVSS Process

- The CVSS process uses a tool called the CVSS v3.1 Calculator.
- The calculator is like a questionnaire in which the choices are made that describe the vulnerability for each metric group.
- Later, a score is generated and numeric severity rating is displayed.

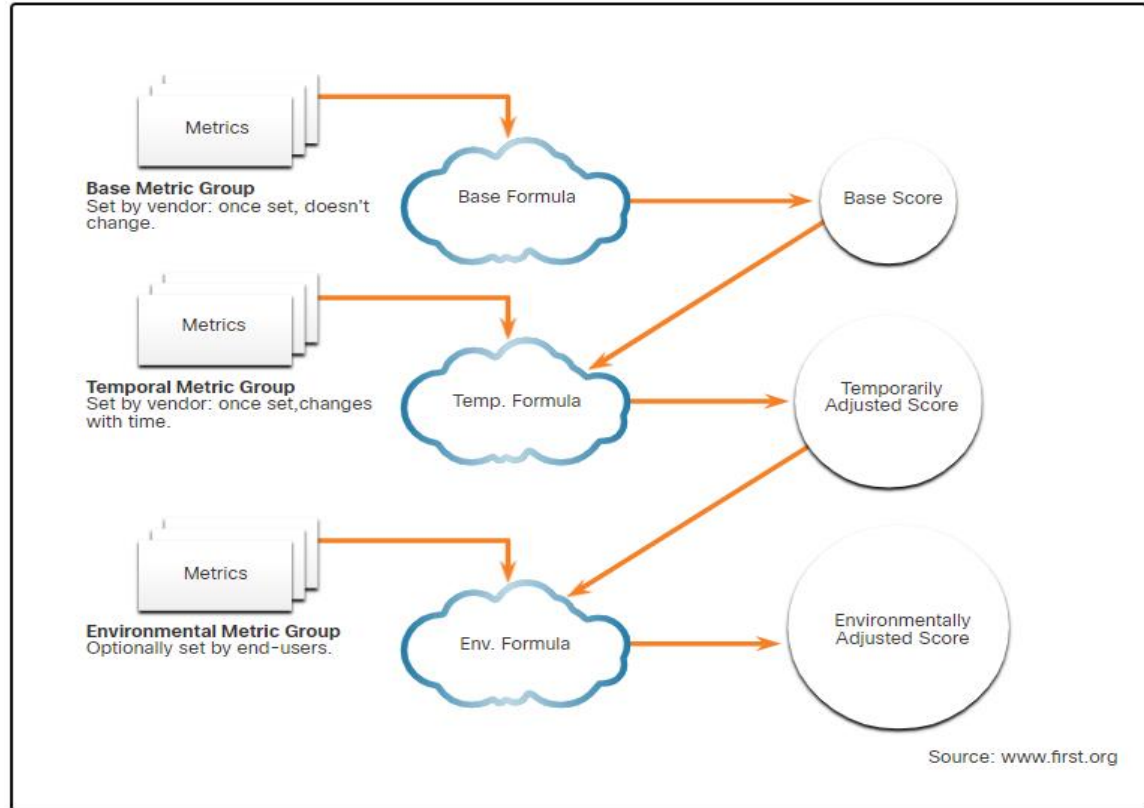
The screenshot displays the CVSS v3.1 Calculator interface. At the top right, a yellow box shows the **Base Score** as **3.8** with a **[Low]** severity rating. Below this, the calculator is organized into two columns of metric groups, each with radio button options:

- Attack Vector (AV):** Network (N) is selected; other options are Adjacent (A), Local (L), and Physical (P).
- Attack Complexity (AC):** Low (L) is selected; other option is High (H).
- Privileges Required (PR):** High (H) is selected; other options are None (N) and Low (L).
- User Interaction (UI):** None (N) is selected; other option is Required (R).
- Scope (S):** Unchanged (U) is selected; other option is Changed (C).
- Confidentiality (C):** Low (L) is selected; other options are None (N) and High (H).
- Integrity (I):** Low (L) is selected; other options are None (N) and High (H).
- Availability (A):** None (N) is selected; other options are Low (L) and High (H).

At the bottom, a green bar displays the **Vector String**: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:A/N

The CVSS Process (Contd.)

- After the Base Metric group is completed, the Temporal and Environmental metric values modify the Base Metric results to provide an overall score.



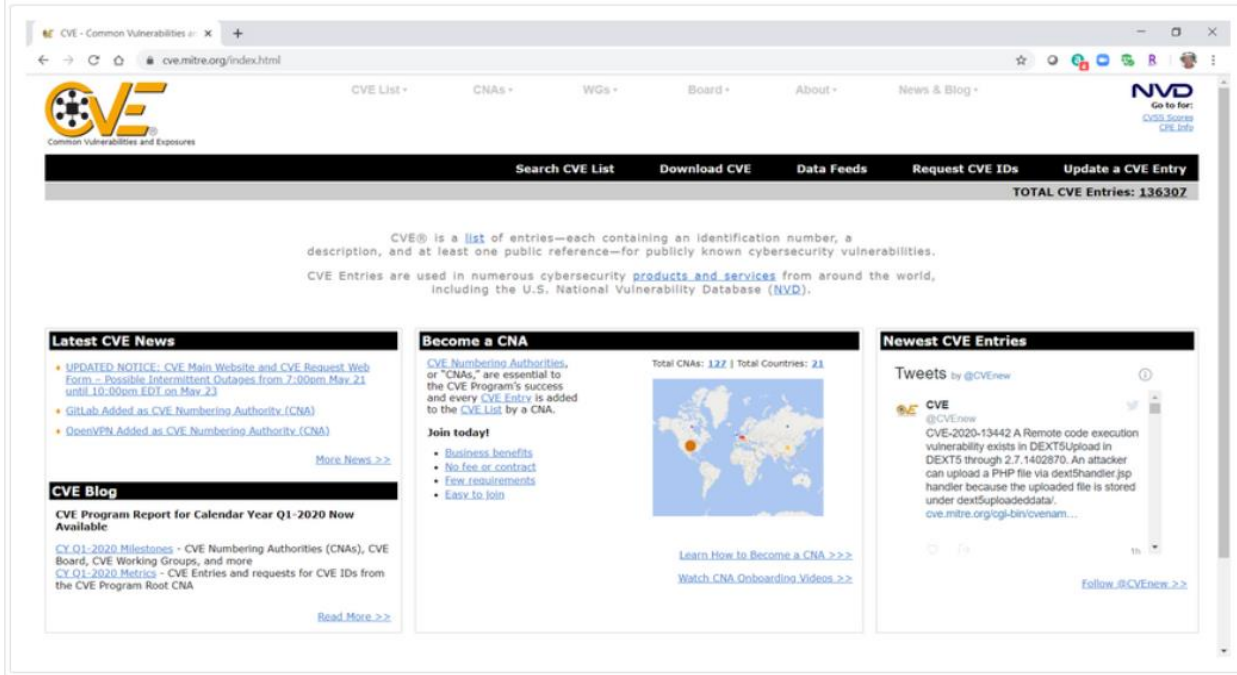
CVSS Reports

- The higher the severity rating, the greater the potential impact of an exploit and the greater the urgency in addressing the vulnerability.
- Any vulnerability that exceeds 3.9 should be addressed.
- The ranges of scores and the corresponding qualitative meaning is shown in the table:

Rating	CVSS Score
None	0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

Other Vulnerability Information Sources

- Common Vulnerabilities and Exposures (CVE):
- CVE identifier provides a standard way to research a reference to vulnerabilities.
- Threat intelligence services use CVE identifiers, and they appear in various security system logs.
- The CVE Details website provides a linkage between CVSS scores and CVE information.



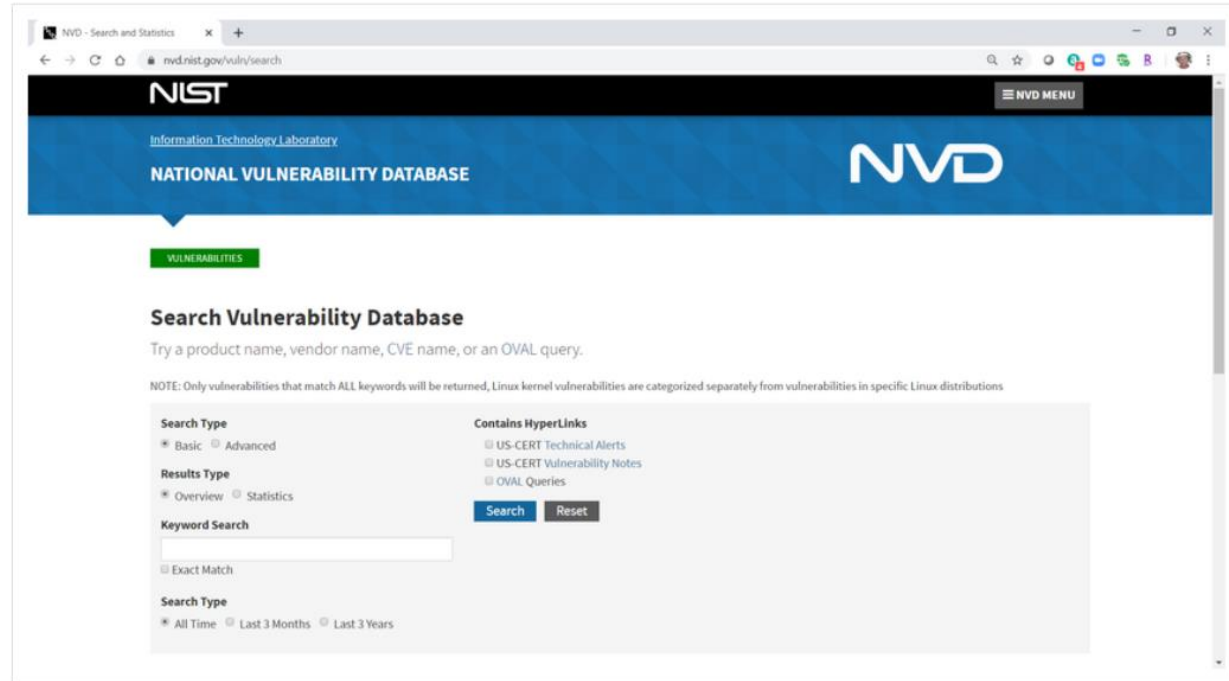
The screenshot shows the CVE website homepage. At the top, there is a navigation bar with links for "CVE List", "CNAs", "WGs", "Board", "About", and "News & Blog". A search bar is located in the center, with buttons for "Search CVE List", "Download CVE", "Data Feeds", "Request CVE IDs", and "Update a CVE Entry". The total number of CVE entries is displayed as 136307. Below the navigation bar, there is a brief description of CVE: "CVE® is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities. CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD)."

The main content area is divided into three columns:

- Latest CVE News:** Contains several news items, including "UPDATED NOTICE: CVE Main Website and CVE Request Web Form - Possible Intermittent Outages from 7:00pm May 21 until 10:00pm EDT on May 21", "GitLab Added as CVE Numbering Authority (CNA)", and "DoveVPN Added as CVE Numbering Authority (CNA)". A "More News >>" link is provided.
- Become a CNA:** Explains that CVE Numbering Authorities (CNAs) are essential to the CVE Program's success and every CVE Entry is added to the CVE List by a CNA. It includes a "Join today!" section with bullet points: "Business benefits", "No fee or contract", "Few requirements", and "Easy to join". A world map shows the locations of CNAs, with a total of 122 in 21 countries. Links for "Learn How to Become a CNA >>>" and "Watch CNA Onboarding Videos >>>" are provided.
- Newest CVE Entries:** Features a tweet from @CVEnew about CVE-2020-13442, a remote code execution vulnerability in DEXt5Upload in DEXt5 through 2.7.1402870. The tweet includes a link to follow #CVEnew >>>.

Other Vulnerability Information Sources (Contd.)

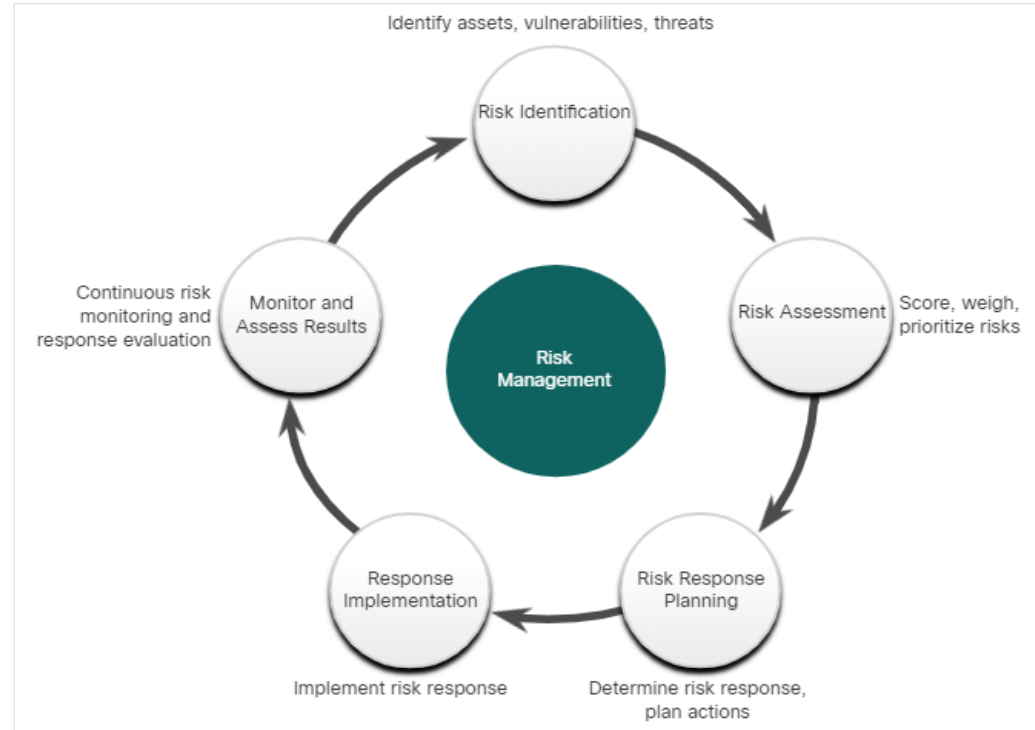
- National Vulnerability Database (NVD):
- This utilizes CVE identifiers and supplies additional information on vulnerabilities such as CVSS threat scores, technical details, affected entities, and resources for further investigation.
- The database was created and is maintained by the U.S. government National Institute of Standards and Technology (NIST) agency.



23.3 Secure Device Management

Risk Management

- Risk management involves the selection and specification of security controls for an organization.
- A mandatory activity in risk assessment is to identify threats and vulnerabilities.
- Ways to respond to identified risks:
 - Risk avoidance - Stop performing the activities that create risk.
 - Risk reduction - Take measures to reduce vulnerability.
 - Risk sharing - Shift some risk to other parties.
 - Risk retention - Accept the risk and its consequences.



Vulnerability Management

- Vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities.
- The steps in the Vulnerability Management Life Cycle:
 - Discover - Develop a network baseline. Identify security vulnerabilities on a regular automated schedule.
 - Prioritize Assets - Categorize assets into groups or business units, and assign a business value based on their criticality to business operations.
 - Assess - Determine a baseline risk profile to eliminate risks based on asset criticality, vulnerability, threats, and asset classification.



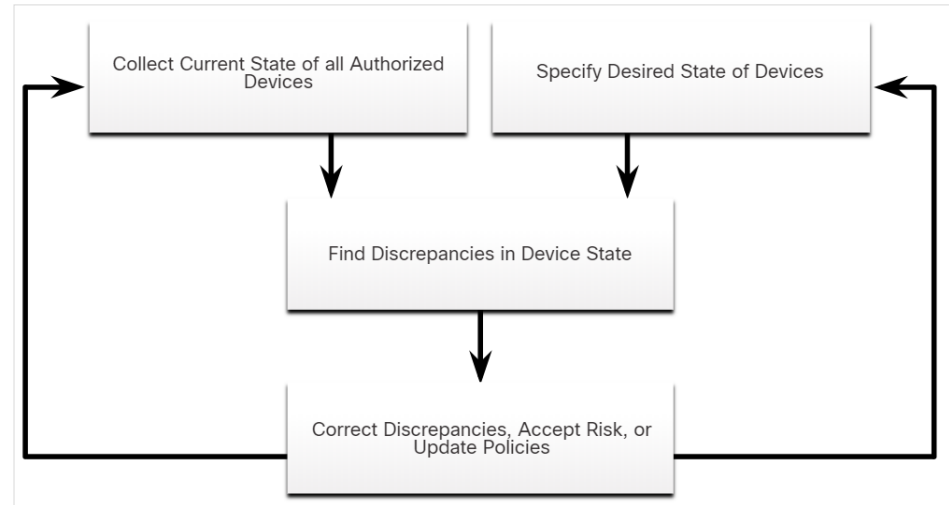
Vulnerability Management (Contd.)

- Report - Measure the level of business risk associated with your assets according to your security policies. Document a security plan, monitor suspicious activity, and describe known vulnerabilities.
- Remediate - Prioritize according to business risk and address vulnerabilities in order of risk.
- Verify - Verify that threats have been eliminated through follow-up audits.



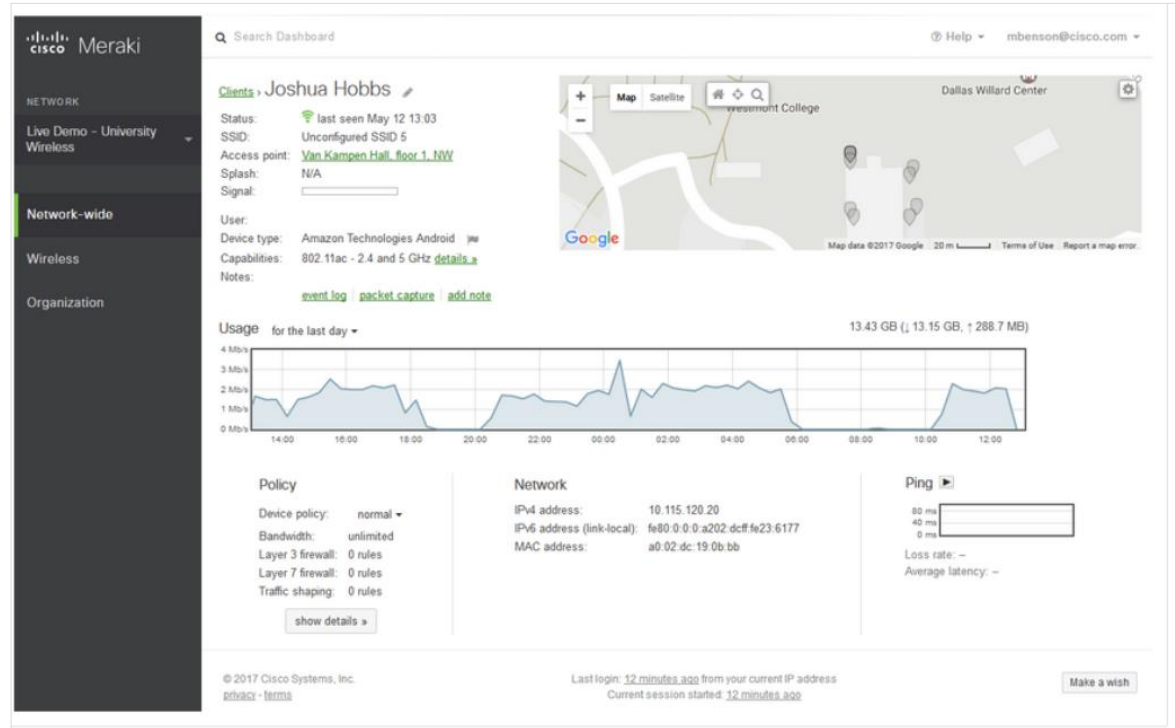
Asset Management

- Asset management involves the implementation of systems that track the location and configuration of networked devices and software across an enterprise.
- **Tools and Techniques for Asset management:**
 - Automated discovery and inventory of the actual state of devices
 - Articulation of the desired state for those devices using policies, plans, and procedures in the organization's information security plan
 - Identification of non-compliant authorized assets
 - Remediation or acceptance of device state, possible iteration of desired state definition
 - Repeat the process at regular or ongoing intervals



Mobile Device Management

- Mobile devices cannot be physically controlled on the premises of an organization.
- MDM systems, such as Cisco Meraki Systems Manager, allows the security personnel to configure, monitor and update a very diverse set of mobile clients from the cloud.

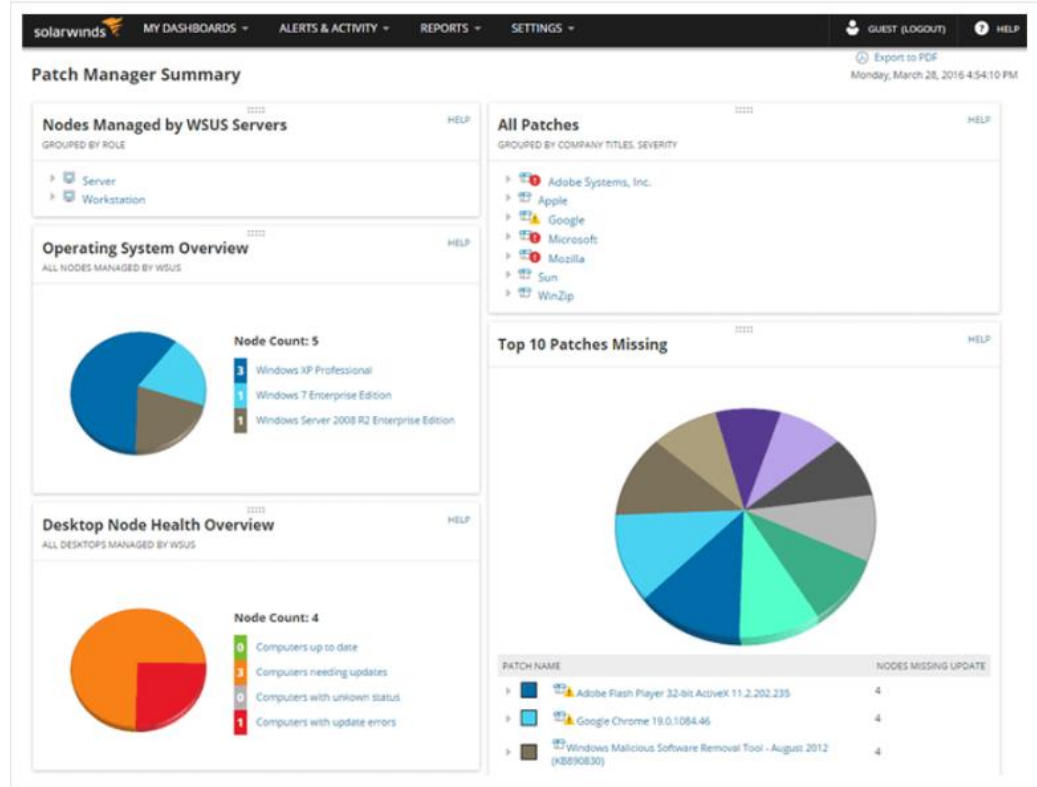


Configuration Management

- Configuration Management: As defined by NIST, configuration management:
- Comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems.
- Configuration tools : Puppet, Chef, Ansible, and SaltStack

Enterprise Patch Management

- Patch management involves all aspects of software patching, including identifying required patches, acquiring, distributing, installing, and verifying.
- Patch management is required by some compliance regulations such as Sarbanes Oxley (SOX) and the Health Insurance Portability and Accountability Act (HIPAA).

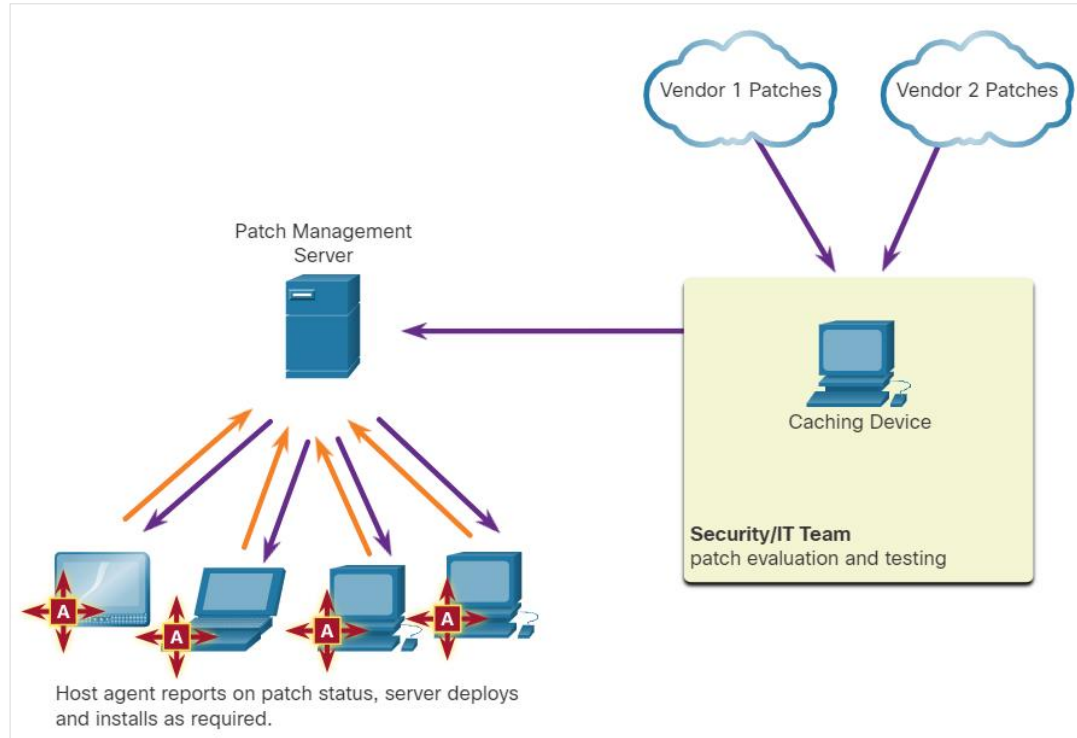


Secure Device Management

Patch Management Techniques

▪ Agent-based:

- This requires a software agent to be running on each host to be patched.
- The agent reports whether vulnerable software is installed on the host.
- The agent communicates with the patch management server and determines if patches exist that require installation, and installs the patches.
- Agent-based approaches are the preferred means of patching mobile devices.

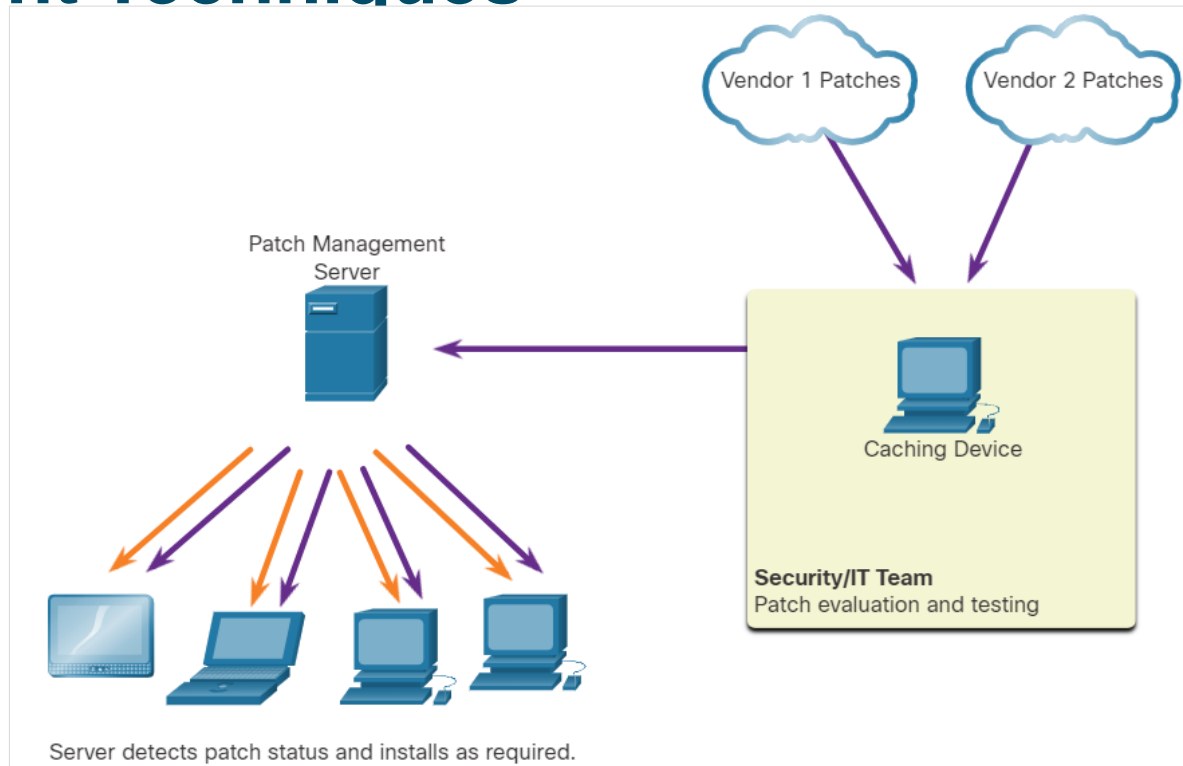


Secure Device Management

Patch Management Techniques

▪ Agentless Scanning:

- Patch management servers scan the network for devices that require patching.
- The server determines which patches are required and installs those patches on the clients.
- Only devices that are on scanned network segments can be patched, which can be a problem for mobile devices.

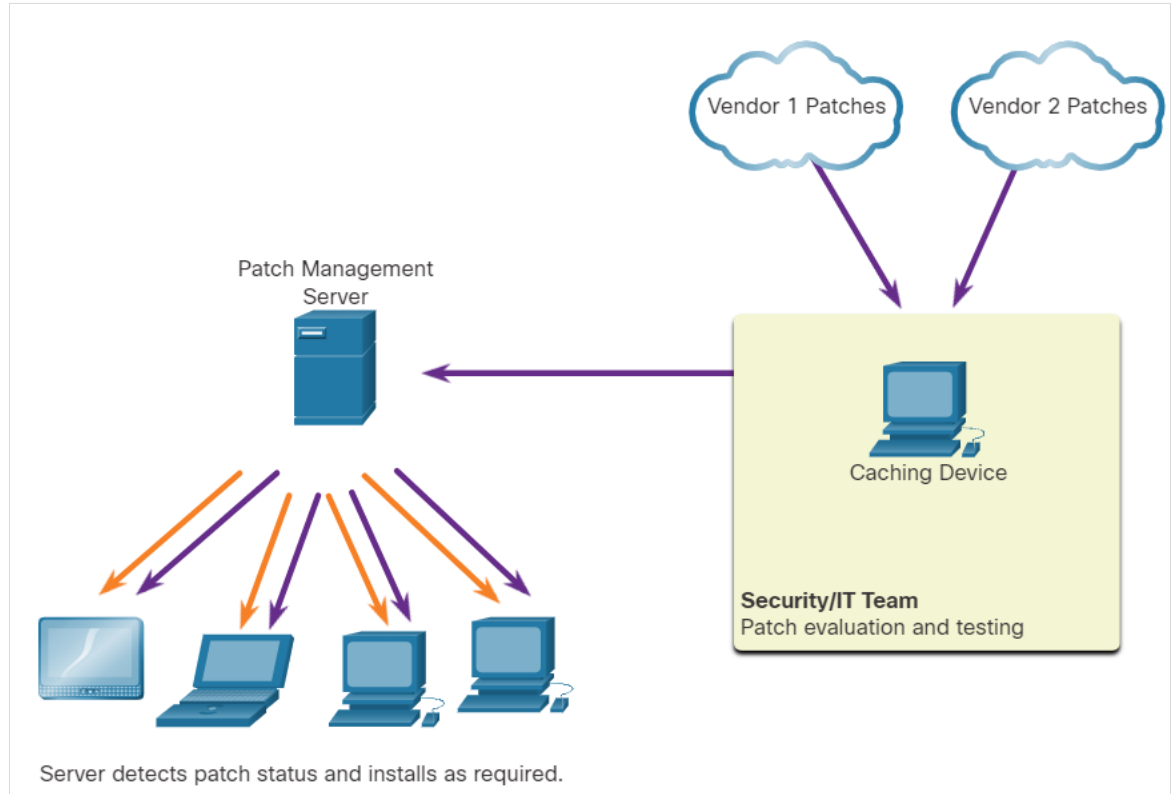


Secure Device Management

Patch Management Techniques

■ Passive Network Monitoring:

- Devices requiring patching are identified through the monitoring of traffic on the network.
- This approach is only effective for software that includes version information in its network traffic.

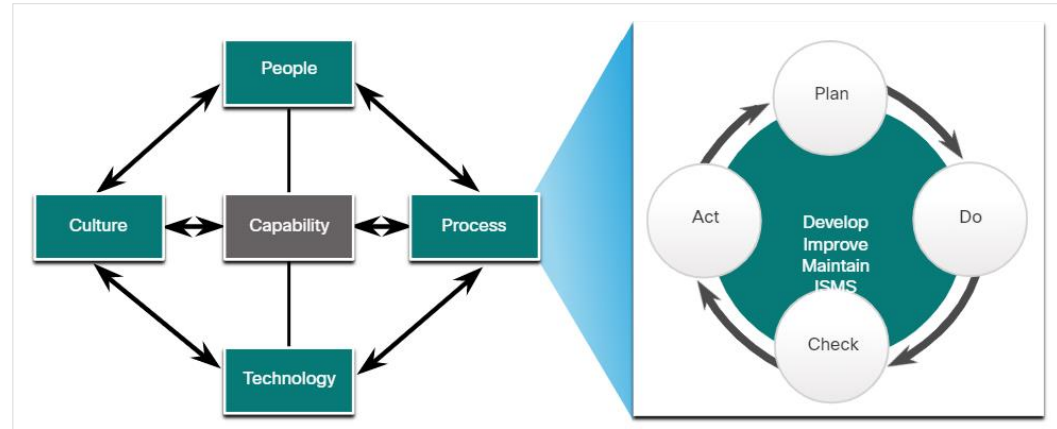


23.4 Information Security Management Systems

Information Security Management Systems

Security Management Systems

- An Information Security Management System (ISMS) consists of a management framework to identify, analyze, and address information security risks.
- ISMSs provide conceptual models that guide organizations in planning, implementing, governing, and evaluating information security programs.
- It incorporates the “plan-do-check-act” framework, known as the Deming cycle.
- ISM is seen as an elaboration on People-Process-Technology-Culture model of organizational capability

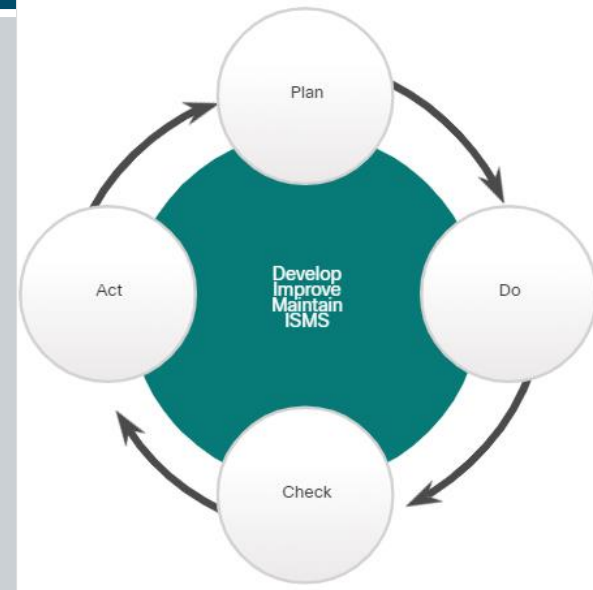


A General Model for Organizational Capability

Information Security Management Systems ISO-27001

- ISO/IEC 27000 family of standards – internationally accepted standards that facilitate business conducted between countries. The ISO 27001 - global, industry-wide specification for an ISMS.

Plan	Do	Check	Act
<ul style="list-style-type: none">Understand business objectivesDefine activities scopeAccess and manage supportAssess and define riskPerform asset management and vulnerability assessment	<ul style="list-style-type: none">Create and implement risk management planEstablish and enforce risk management policies and proceduresTrain personnel, allocate resources	<ul style="list-style-type: none">Monitor executionCompile reportsSupport external certification audit	<ul style="list-style-type: none">Continually audit processesContinually improve processesTake corrective actionTake preventive action



Information Security Management Systems

NIST Cybersecurity Framework

- NIST Cybersecurity Framework – is a set of standards designed to integrate existing standards, guidelines, and practices to help better manage and reduce cybersecurity risk.
- The below table describes the core functions in NIST Cybersecurity Framework:

Core Function	Description
IDENTIFY	Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
PROTECT	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
DETECT	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
RESPOND	Develop and implement the appropriate activities to act on a detected cybersecurity event.
RECOVER	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

23.5 Endpoint Vulnerability Assessment Summary

Endpoint Vulnerability Assessment

Endpoint Vulnerability Assessment Summary

- Network and device profiling provides statistical baseline information that can serve as a reference point for normal network and device performance.
- Network security can be evaluated using a variety of tools and services.
- Vulnerability assessment uses software to scan Internet-facing servers and internal networks for various types of vulnerabilities.
- The Common Vulnerability Scoring System (CVSS) is a vendor-neutral, industry standard, open framework for rating the risks of a given vulnerability by using a variety of metrics to calculate a composite score.
- Vulnerabilities are rated according to the attack vector, attack complexity, privileges required, user interaction, and scope.
- Risk management involves the selection and specification of security controls for an organization.

Endpoint Vulnerability Assessment Summary

(Contd.)

- Vulnerability management is a security practice that is designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization.
- Organizations can use an Information Security Management System (ISMS) to identify, analyze, and address information security risks.
- Standards for managing cybersecurity risk are available from ISO and NIST.
- NIST has also developed the Cybersecurity Framework, which is similar to the ISO/IEC 27000 standards.

Thank you! Questions?



Vladimír Veselý

updated: 2023-03-27

<https://www.fit.vutbr.cz/research/groups/nes@fit>