

Knowledge Check Activity 1

Which of the following is the beginning point of a certificate chain?

- a. User certificate
- b. Intermediate certificate
- c. Root certificate
- d. Top-level certificate

Knowledge Check Activity 1: Answer

Which of the following is the beginning point of a certificate chain?

Answer: c. Root certificate

The beginning point of a certificate chain is the root certificate and they do not depend on a higher-level authority.

Public Key Infrastructure (PKI)

- PKI is one of the most important management tools for the use of:
 - Digital certificates:
 - Asymmetric cryptography
- It is important to understand PKI:
 - Know PKI trust models
 - How it is managed
 - Features of key management

What is Public Key Infrastructure (PKI)?

- There is a need for a consistent means to manage digital certificates
- **Public key infrastructure (PKI)** is a framework for all entities involved in digital certificates
- Certificate management actions facilitated by PKI
 - Create
 - Store
 - Distribute
 - Revoke

Trust Models (1 of 3)

- *Trust* is defined as confidence in or reliance on another person or entity
- A **trust model** refers to the type of trust relationship that can exist between individuals and entities
- *Direct trust* is a type of trust model where one person knows the other person
- *Third-party trust* refers to a situation where two individuals trust each other because each trusts a third party
- The web of trust model is based on direct trust
 - Each user signs a digital certificate then exchanges certificates with all other users
- Three PKI trust models use a CA:
 - The hierarchical trust model, the distributed trust model, and the bridge trust model

Trust Models (2 of 3)

- Hierarchical Trust Model
 - The *hierarchical trust model* assigns a single hierarchy with one master CA called *root*
 - The root signs all digital certificate authorities with a single key
 - This model can be used in an organization where one CA is responsible for only that organization's digital certificates
 - Hierarchical trust model limitations:
 - A single CA private key may be compromised rendering all certificates worthless
 - Having a single CA who must verify and sign all digital certificates may create a significant backlog
- Distributed Trust Model
 - The *distributed trust model* has multiple CAs that sign digital certificates
 - Eliminates limitations of hierarchical trust model

Trust Models (3 of 3)

- Bridge Trust Model
 - The *bridge trust model* is similar to the distributed trust model
 - One CA acts as a *facilitator* to interconnect connect all other CAs
 - Facilitator CA does not issue digital certificates, instead it acts as hub between hierarchical and distributed trust model
 - Allows the different models to be linked

Managing PKI (1 of 2)

- Certificate Policy (CP)
 - A *certificate policy (CP)* is a published set of rules that govern operation of a PKI
 - The CP provides recommended baseline security requirements for the use and operation of CA, RA, and other PKI components
- Certificate Practice Statement (CPS)
 - A *certificate practice statement* is a technical document that describes in detail how the CA uses and manages certificates
 - It also covers how to register for a digital certificate, how to issue them, when to revoke them, procedural controls and key pair management

Managing PKI (2 of 2)

- Certificate Life Cycle
 - *Creation*
 - Occurs after user is positively identified
 - *Suspension*
 - May occur when employee on leave of absence
 - *Revocation*
 - Certificate no longer valid
 - *Expiration*
 - Key can no longer be used

Key Management (1 of 2)

- Key Storage
 - Public keys can be stored by embedding them within digital certificates
 - Private keys can be stored on user's local system
 - Software-based storage may expose keys to attackers
 - Alternative: storing keys in hardware
 - Smart-cards
 - Tokens
- Key Usage
 - Multiple pairs of dual keys can be created
 - One pair is used to encrypt information and the public key backed up in another location
 - Second pair would be used only for digital signatures and the public key in that pair would never be backed up

Key Management (2 of 2)

- Key Handling Procedures
 - *Escrow*
 - *Expiration*
 - *Renewal*
 - *Revocation*
 - *Recovery*
 - *Suspension*
 - *Destruction*

Knowledge Check Activity 2

Which of the following is considered a non-secure place where PKI encryption keys may be stored?

- a. Smart-card
- b. Token
- c. In a digital certificate
- d. Local system

Knowledge Check Activity 2: Answer

Which of the following is considered a non-secure place where PKI encryption keys may be stored?

Answer: d. Local system

Private keys can be stored on a user's local system but this can leave keys open to attacks due to possible vulnerabilities in the OS. Storing keys in hardware such as tokens and smart-cards is usually a more secure alternative.

Cryptographic Protocols

- The most common cryptographic transport algorithms include the following:
 - Secure Sockets Layer
 - Transport Layer Security
 - Secure Shell
 - Hypertext Transport Protocol Secure
 - S/MIME
 - Secure Real-time Transport Protocol
 - IP Security

Secure Sockets Layer (SSL)

- **Secure Sockets Layer (SSL)** is one of the most common cryptographic protocols
 - Developed by Netscape in 1994
 - The design goal was to create an encrypted data path between a client and a server
 - SSL uses the Advanced Encryption Standard (AES)
 - SSL version 3.0 is the current version

Transport Layer Security (TLS)

- **Transport Layer Security (TLS)** is a replacement for SSL
 - Versions starting with v1.1 are significantly more secure than SSL v3.0
 - Current version is TLS v1.2
 - A *cipher suite* is a named combination of the encryption, authentication, and message authentication code (MAC) algorithms that are used with SSL and TLS

Secure Shell (SSH)

- **Secure Shell (SSH)** is an encrypted alternative to the Telnet protocol used to access remote computers
- It is a Linux/UNIX-based command interface and protocol
- SSH is a suite of three utilities: *slogin*, *ssh*, and *scp*
- Client and server ends of the connection are authenticated using a digital certificate and passwords are encrypted
- SSH can be used as a tool for secure network backups

Hypertext Transport Protocol Secure (HTTPS)

- A common use of TLS and SSL is to secure **Hypertext Transport Protocol (HTTP)** communications between a browser and Web server
- The secure version is actually “*plain*” HTTP sent over SSL or TLS and is called Hypertext Transport Protocol Secure (HTTPS)
- HTTPS uses port 443 instead of HTTP’s port 80
- Users must enter URLs with https://

Secure/Multipurpose Internet Mail Extensions (S/MIME)

- **Secure/Multipurpose Internet Mail Extensions (S/MIME)** is a protocol for securing email messages
- MIME is a standard for how an electronic message will be organized, so S/MIME describes how encryption information and a digital certificate can be included as part of the message body
- S/MIME allows users to send encrypted messages that are also digitally signed

Secure Real-time Transport Protocol (SRTP)

- **Secure Real-time Transport Protocol (SRTP)** is a secure extension protecting transmission using the Real-time Transport Protocol (RTP)
- SRTP provides protection for Voice over IP (VoIP) communications
- Adds security features such as message authentication and confidentiality for VoIP Communications

IP Security (IPsec)

- **IPsec** is a protocol suite for securing Internet Protocol (IP) communications
- IPsec is considered to be a *transparent* security protocol
 - Transparent to applications, users, and software
- IPsec provides three areas of protection that correspond to three IPsec protocols:
 - *Authentication*
 - *Confidentiality*
 - *Key management*
- IPsec supports two encryption modes:
 - **Transport mode** encrypts only the data portion of each packet and leaves the header unencrypted
 - **Tunnel mode** encrypts both the header and the data portion

Weaknesses of Cryptographic Protocols

- Due to the complexity of networking, cryptographic protocols are notoriously difficult to design
- While the mathematics and related security of basic cryptographic algorithms have been extensively studied, the same cannot be said of cryptographic protocols
- Older cryptographic protocols were designed by networking experts and not by cryptographic protocol experts
- The associated security proofs to guarantee the correctness of cryptographic protocols are much more complicated than those for cryptographic algorithms

Knowledge Check Activity 3

Which encryption protocol is used for securing email messages?

- a. S/MIME
- b. SRTP
- c. HTTPS
- d. TLS

Knowledge Check Activity 3: Answer

Which encryption protocol is used for securing email messages?

Answer: a. S/MIME

Secure/Multipurpose Internet Mail Extensions (S/MIME) is used to secure email messages. SRTP provides VOIP protection, HTTPS is used, along with TLS, to secure communication between a Web browser and Web server.

Implementing Cryptography

- Cryptography that is improperly applied can lead to vulnerabilities
- It is essential to understand the different options that relate to cryptography
- Implementing cryptography includes understanding:
 - Key strength
 - Secret algorithms
 - Block cipher modes of operation
 - Cryptographic service providers
 - The use of algorithm input values

Key Strength

- A cryptographic key is a value that serves as input to an algorithm
 - It transforms plaintext into ciphertext (and vice versa for decryption)
- Three primary characteristics that determine the resiliency of the key to attacks (called **key strength**)
 - *Randomness*
 - *Length of the key*
 - *Cryptoperiod* – length of time for which a key is authorized for use

Secret Algorithms

- Keys must be kept secret, does the same apply to algorithms?
- Would a secret algorithm enhance security in the same way as keeping a key or password secret?
 - No
- For a cryptography to be useful it needs to be widespread:
 - A military force that uses cryptography must allow many users to know of its existence to use it

Block Cipher Modes of Operation

- A *block cipher* manipulates an entire block of plaintext at one time
 - The plaintext is divided into separate blocks of specific lengths
 - Each block is encrypted independently
- A block cipher mode of operation specifies how block ciphers should handle these blocks
- Most common modes:
 - *Electronic Code Book (ECB)*
 - *Cipher Block Chaining (CBC)*
 - *Counter (CTR)*
 - *Galois/Counter (GCM)*

Crypto Service Providers

- A *crypto service provider* allows an application to implement an encryption algorithm for execution
- Crypto service providers typically:
 - Implement cryptographic algorithms
 - Generate keys
 - Provide key storage
 - Authenticate users by calling various crypto modules to perform specific tasks
- Crypto service providers can be implemented in:
 - Software, hardware, or both

Knowledge Check Activity 4

Which of the following is NOT a primary characteristic of key strength?

- a. Randomness
- b. Uniqueness
- c. Key length
- d. Cryptoperiod

Knowledge Check Activity 4: Answer

Which of the following is NOT a primary characteristic of key strength?

Answer: b. Uniqueness

The three primary characteristics that determine the resiliency of the key to attacks, or key strength, are: randomness, length of key, and cryptoperiod.

Self-Assessment

Do case projects 7-3 and 7-4 which relate to Certificate Authorities. Then consider the following questions: How important is the CA from which you purchase a digital certificate? What are the ramifications of using a certificate from an unreliable source?

Summary (1 of 2)

- A digital certificate is the user's public key that has been digitally signed by a trusted third party who verifies the owner and that the public key belongs to that owner
- A Certificate Repository (CR) is a list of approved digital certificates
- The process of verifying that a digital certificate is genuine depends upon certificate chaining, or linking several certificates together to establish trust between all the certificates involved
- Domain validation digital certificates verify the identity of the entity that has control over the domain name but indicate nothing regarding the trustworthiness of the individuals behind the site
- A public key infrastructure (PKI) is the underlying infrastructure for key management of public keys and digital certificates

Summary (2 of 2)

- An organization that uses multiple digital certificates on a regular basis needs to properly manage those digital certificates
- Cryptography is commonly used to protect data in transit/motion
- Cryptography that is improperly applied can lead to vulnerabilities that will be exploited