Instructor Materials
Chapter 4: The Art of Protecting Secrets

Cybersecurity Essentials v1.1

Cisco | Networking Academy®
Mind Wide Open™

Chapter 4: The Art of Protecting Secrets

Cybersecurity Essentials v1.1

Cisco | Networking Academy®
Mind Wide Open™

Chapter 4 - Sections & Objectives

4.1 Cryptography

Explain how encryption techniques protect confidentiality.

4.2 Access Control

Describe access control techniques used to protect confidentiality.

4.3 Obscuring Data

Describe the concept of obscuring data.

4.1 Cryptography

Cisco | Networking Academy®
Mind Wide Open™

Cryptography
Overview

Cryptology is the science of making and breaking secret codes. Cryptography is a way to store and transmit data so only the intended recipient can read or process it. Modern cryptography uses computationally secure algorithms to make sure that cyber criminals cannot easily compromise protected information.

The history of cryptography started in diplomatic circles thousands of years ago. Messengers from a king's court took encrypted messages to other courts. Occasionally, other courts not involved in the communication, attempted to steal messages sent to a kingdom they considered an adversary. Not long after, military commanders started using encryption to secure messages.

Each encryption method uses a specific algorithm, called a cipher, to encrypt and decrypt messages. A cipher is a series of well-defined steps used to encrypt and decrypt messages. There are several methods of creating ciphertext:

- Transposition
- Substitution
- One-time pad

Overview (Cont.)

Two Types of Encryption

There are two classes of encryption algorithms:

- **Symmetric algorithms** - These algorithms use the same pre-shared key, sometimes called a secret key pair, to encrypt and decrypt data. Both the sender and receiver know the pre-shared key before any encrypted communication begins.
- **Asymmetric algorithms** - Asymmetrical encryption algorithms use one key to encrypt data and a different key to decrypt data. One key is public and the other is private. In a public-key encryption system, any person can encrypt a message using the public key of the receiver, and the receiver is the only one that can decrypt it using his private key. Parties exchange secure messages without needing a pre-shared key. Asymmetric algorithms are more complex. These algorithms are resource intensive and slower to execute.

Private-Key Encryption

Symmetrical Encryption Process - Symmetric algorithms use pre-shared key to encrypt and decrypt data, a method also known as private-key encryption. Numerous encryption systems use symmetric encryption. Some of the common encryption standards that use symmetric encryption include the following:

- **3DES (Triple DES):** Digital Encryption Standard (DES) is a symmetric block cipher with 64-bit block size that uses a 56-bit key. Triple DES encrypts data three times and uses a different key for at least one of the three passes, giving it a cumulative key size of 112-168 bits.
- **IDEA:** The International Data Encryption Algorithm (IDEA) uses 64-bit blocks and 128-bit keys. IDEA performs eight rounds of transformations on each of the 16 blocks that results from dividing each 64-bit block. IDEA was the replacement for DES, and now PGP (Pretty Good Privacy) uses it.
- **AES:** The Advanced Encryption Standard (AES) has a fixed block size of 128-bits with a key size of 128, 192, or 256 bits. The National Institute of Standards and Technology (NIST) approved the AES algorithm in December 2001. The U.S. government uses AES to protect classified information.

Public-Key Encryption

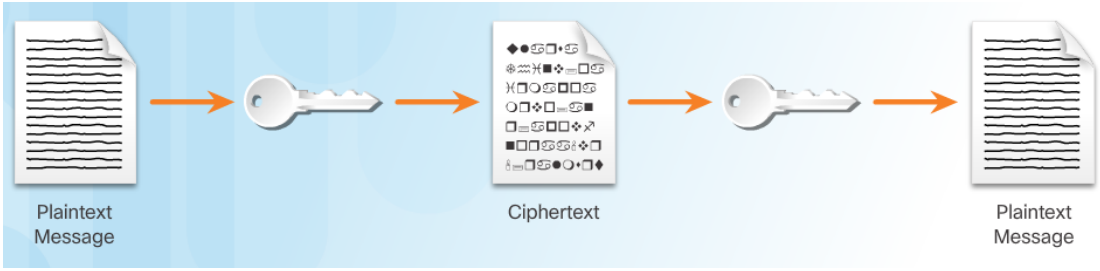
Asymmetrical Encryption Process - Asymmetric encryption, also called public-key encryption, uses one key for encryption that is different from the key used for decryption. A criminal cannot calculate the decryption key based on knowledge of the encryption key, and vice versa, in any reasonable amount of time. The asymmetric algorithms include:

- **RSA (Rivest_Shamir-Adleman)** - uses the product of two very large prime numbers with an equal length of between 100 and 200 digits. Browsers use RSA to establish a secure connection.
- **Diffie-Hellman** - provides an electronic exchange method to share the secret key. Secure protocols, such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH), and Internet Protocol Security (IPsec), use Diffie-Hellman.
- **ElGamal** - uses the U.S. government standard for digital signatures. This algorithm is free to use because no one holds the patent.
- **Elliptic Curve Cryptography (ECC)** - uses elliptic curves as part of the algorithm. In the U.S., the National Security Agency uses ECC for digital signature generation and key exchange.

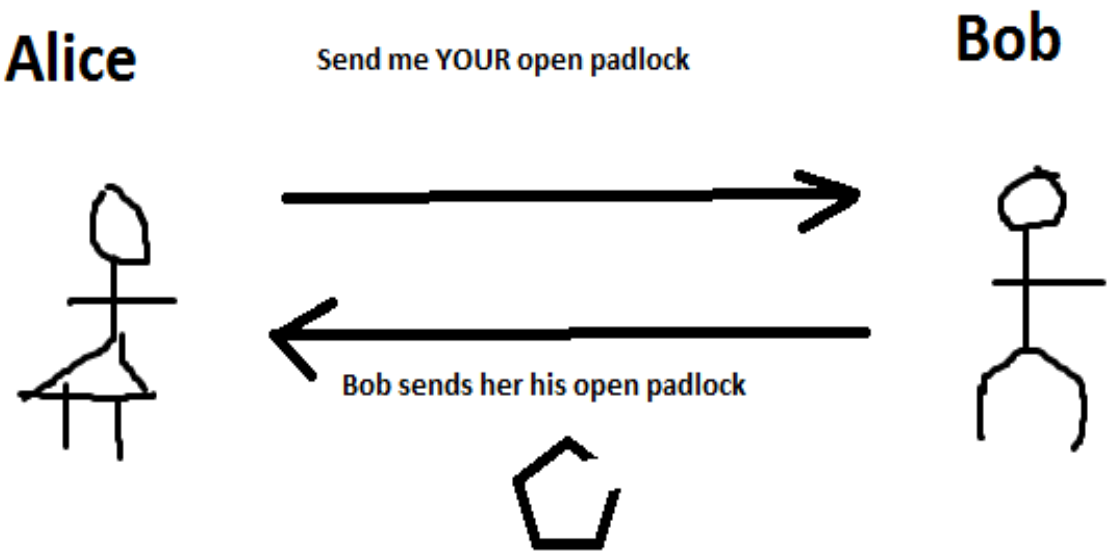
Symmetrical versus Asymmetrical Encryption

Comparing Encryption Types

- It is important to understand the differences between symmetric and asymmetric encryption methods. Symmetric encryption systems are more efficient and can handle more data. However, key management with symmetric encryption systems is more problematic and harder to manage.
- Asymmetric cryptography is more efficient at protecting the confidentiality of small amounts of data, and its size and speed make it more secure for tasks such as electronic key exchange which is a small amount of data rather than encrypting large blocks of data.



Asymmetric Encryption



Symmetrical versus Asymmetrical Encryption

Application

There are many applications for both symmetric and asymmetric algorithms. A one-time password-generating token is a hardware device that uses cryptography to generate a one-time password. A one-time password is an automatically generated numeric or alphanumeric string of characters that authenticates a user for one transaction of one session only. The number changes every 30 seconds or so. The session password appears on a display and the user enters the password.

- The electronic payment industry uses 3DES.
- Operating systems use DES to protect user files and system data with passwords.
- Most encrypting file systems, such as NTFS, use AES.

Symmetrical versus Asymmetrical Encryption

Application

Four protocols use asymmetric key algorithms:

- Internet Key Exchange (IKE), which is a fundamental component of IPsec Virtual Private Networks (VPNs).
- Secure Socket Layer (SSL), which is a means of implementing cryptography into a web browser.
- Secure Shell (SSH), which is a protocol that provides a secure remote access connection to network devices.
- Pretty Good Privacy (PGP), which is a computer program that provides cryptographic privacy and authentication to increase the security of email communications.

Symmetrical versus Asymmetrical Encryption

Application

A VPN is a private network that uses a public network, usually the Internet, to create a secure communication channel. A VPN connects two endpoints such as two remote offices over the Internet to form the connection.

- VPNs use IPsec. IPsec is a suite of protocols developed to achieve secure services over networks.
- IPsec services allow for authentication, integrity, access control, and confidentiality.
- With IPsec, remote sites can exchange encrypted and verified information.
- Data in use is a growing concern to many organizations. When in use, data no longer has any protection because the user needs to open and change the data.
- System memory holds data in use and it can contain sensitive data such as the encryption key.
- If criminals compromise data in use, they will have access to data at rest and data in motion.

4.2 Access Control

Cisco | Networking Academy®
Mind Wide Open™

Types of Access Control

Physical Access Controls - actual barriers deployed to prevent direct contact with systems. The goal is to prevent unauthorized users from gaining physical access to facilities, equipment, and other organizational assets. Physical access control determines who can enter (or exit), where they can enter (or exit), and when they can enter (or exit).

Logical Access Controls - hardware and software solutions used to manage access to resources and systems. These technology-based solutions include tools and protocols that computer systems use for identification, authentication, authorization, and accountability.

Administrative Access Controls - policies and procedures defined by organizations to implement and enforce all aspects of controlling unauthorized access. Administrative controls focus on personnel and business practices.

Access Control Strategies

Mandatory access control (MAC) - restricts the actions that a subject can perform on an object. A subject can be a user or a process. An object can be a file, a port, or an input/output device. An authorization rule enforces whether or not a subject can access the object.

Discretionary access control (DAC) - DAC grants or restricts object access determined by the object's owner. As the name implies, controls are discretionary because an object owner with certain access permissions can pass on those permissions to another subject.

Role-based access control (RBAC) - is based on the role of the subject. Roles are job functions within an organization. Specific roles require permissions to perform certain operations. Users acquire permissions through their role. RBAC can work in combination with DAC or MAC by enforcing the policies of either one.

Rule-based access control - uses access control lists (ACLs) to help determine whether to grant access. A series of rules is contained in the ACL, as shown in the figure. The determination of whether to grant access depends on these rules. An example of such a rule is one that states that no employee may have access to the payroll file after hours or on weekends.

Identification

Identification enforces the rules established by the authorization policy:

- A subject requests access to a system resource.
- Every time the subject requests access to a resource, the access controls determine whether to grant or deny access.
- Cybersecurity policies determine which identification controls should be used.
- The sensitivity of the information and information systems determine how stringent the controls.
- The increase in data breaches has forced many organizations to strengthen their identification controls.

Authentication Methods

What You Know - Passwords, passphrases, or PINs are all examples of something that the user knows. Passwords are the most popular method used for authentication.

What You Have - Smart cards and security key fobs are both examples of something that users have in their possession.

Who You Are - A unique physical characteristic, such as a fingerprint, retina, or voice, that identifies a specific user is called biometrics.

Multi-factor Authentication - Multi-factor authentication uses at least two methods of verification. A security key fob is a good example. The two factors are something you know, such as a password, and something you have, such as a security key fob.

Authorization

Authorization controls what a user can and cannot do on the network after successful authentication:

- After a user proves his or her identity, the system checks to see what network resources the user can access and what the users can do with the resources.
- Authorization uses a set of attributes that describes the user's access to the network.
- The system compares these attributes to the information contained within the authentication database, determines a set of restrictions for that user, and delivers it to the local router where the user is connected.
- Defining authorization rules is the first step in controlling access. An authorization policy establishes these rules.

Accountability

Accountability traces an action back to a person or process making the change to a system, collects this information, and reports the usage data:

- The organization can use this data for such purposes as auditing or billing.
- The collected data might include the log in time for a user, whether the user log in was a success or failure, or what network resources the user accessed.
- This allows an organization to trace actions, errors, and mistakes during an audit or investigation.
- Implementing accountability consists of technologies, policies, procedures, and education.
- Log files provide detailed information based on the parameters chosen.

Types of Security Controls

Preventative Controls - Prevent means to keep something from happening. Preventative access controls stop unwanted or unauthorized activity from happening.

Deterrent Controls - A deterrent is the opposite of a reward. A reward encourages individuals to do the right thing, while a deterrent discourages them from doing the wrong thing. Cybersecurity professionals and organizations use deterrents to limit or mitigate an action or behavior. Deterrents do not always stop these actions.

Detective Controls - Detection is the act or process of noticing or discovering something. Access control detections identify different types of unauthorized activity. Detection systems can be very simple, such as a motion detector or security guard. They can also be more complex, such as an intrusion detection system.

Types of Security Controls

Corrective Controls - Corrective counteracts something that is undesirable. Organizations put corrective access controls in place after a system experiences a threat. Corrective controls restore the system back to a state of confidentiality, integrity, and availability. They can also restore systems to normal after unauthorized activity occurs.

Recovery Controls - Recovery is a return to a normal state. Recovery access controls restore resources, functions, and capabilities after a violation of a security policy. Recovery controls can repair damage, in addition to stopping any further damage. These controls have more advanced capabilities over corrective access controls.

Compensative Controls - Compensate means to make up for something. Compensative access controls provide options to other controls to bolster enforcement in support of a security policy. A compensative control can also be a substitution used in place of a control that is not possible under the circumstances.

4.3 Obscuring Data

Cisco | Networking Academy®
Mind Wide Open™

Obscuring Data

Data Masking

Data Masking is a technology that secures data by replacing sensitive information with a non-sensitive version. The non-sensitive version looks and acts like the original. This means that a business process can use non-sensitive data and there is no need to change the supporting applications or data storage facilities.

In the most common use case, masking limits the propagation of sensitive data within IT systems by distributing surrogate data sets for testing and analysis.

There are data masking techniques that can ensure that data remains meaningful but changed enough to protect it:

- **Substitution** - replaces data with authentic looking values to apply anonymity to the data records.
- **Shuffling** - derives a substitution set from the same column of data that a user wants to mask. This technique works well for financial information in a test database, for example.

Steganography

Steganography conceals data (the message) in another file such as a graphic, audio, or other text file.

The advantage of steganography over cryptography is that the secret message does not attract any special attention. No one would ever know that a picture actually contained a secret message by viewing the file either electronically or in hardcopy.

There are several components involved in hiding data:

- There is the embedded data, which is the secret message.
- Cover-text (or cover-image or cover-audio) hides the embedded data producing the stego-text (or stego-image or stego-audio).
- A stego-key controls the hiding process.

Data Obfuscation

Data obfuscation - is the use and practice of data masking and steganography techniques in the cybersecurity and cyber intelligence profession:

- Obfuscation is the art of making the message confusing, ambiguous, or harder to understand.
- A system may purposely scramble messages to prevent unauthorized access to sensitive information.
- Software watermarking protects software from unauthorized access or modification.
- Software watermarking inserts a secret message into the program as proof of ownership.
- The secret message is the software watermark. If someone tries to remove the watermark, the result is nonfunctional code.

4.4 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

Summary

- This chapter discussed the principles of cryptology used to secure communications.
- The chapter explained both symmetric and asymmetric encryption algorithms, compared the two algorithms, and provided examples of their use.
- The chapter explained how access control prevents unauthorized access to a building, a room, a system, or a file using identification, authentication, authorization, and accountability. In addition, the chapter also described the different access control models and access control types.
- The chapter concluded by discussing the various ways users mask data. Data obfuscation and steganography are two techniques used to accomplish data masking.