Chapter 12 – Cryptography

Notes

Overview

This chapter describes the history of cryptography. It also explains several symmetric and asymmetric cryptography algorithms. You will learn about the similarities and differences between symmetric and asymmetric cryptography. The chapter also explains public key infrastructure (PKI) and when it is appropriate to use. You will learn about possible attacks to cryptosystems and also compare hashing algorithms.

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to:

- Summarize the history and principles of cryptography
- Describe symmetric and asymmetric encryption algorithms
- Explain public key infrastructure (PKI)
- Describe possible attacks on cryptosystems
- Compare hashing algorithms and how they ensure data integrity

Tips

Understanding Cryptography Basics

1. This section will cover basic aspects of cryptography. Cryptography is the process of converting plaintext into ciphertext. Decryption is the process of converting ciphertext into plaintext (also called cleartext).

History of Cryptography

1. Examples of ancient cryptography include the encryption of selected Egyptian hieroglyphics and the cipher used to write the Book of Jeremiah.
2. A substitution cipher is a type of cryptography that replaces one letter with another based on a key. For example, the cipher developed by Julius Caesar encrypted messages by shifting each letter of the alphabet three positions.
3. Cryptanalysis's role is proving that an encryption algorithm cannot be broken or that it will take so much time and resources that it is impractical for hackers to attempt breaking it.

The War Machines

1. Enigma is a substitution ciphering machine developed and used by the Germans during World War II.
2. The Purple Machine is another ciphering machine based on the techniques discovered by Herbert O. Yardley. This machine was used by the Japanese during World War II to secure their communications.
3. Understand steganography.

Tip	Find more information about these machines at the following links: http://www.bbc.co.uk/history/topics/enigma http://www.codesandciphers.org.uk/enigma/

Understanding Symmetric and Asymmetric Algorithms

1. Understand what an algorithm is and how it can be used along with a key to protect confidential data.

2. Understand the importance of selecting a good random key and keeping it secret.

3. See Table 12-1 for the different types of algorithms.

Symmetric Algorithms

1. Symmetric algorithms are algorithms that use the same key for data encryption and decryption.

2. Understand the main advantages and disadvantages of symmetric algorithms.

3. The two types of symmetric algorithms currently in use: stream ciphers and block ciphers.

Data Encryption Standard

1. DES was the result of a contest organized by the National Institute of Standards and Technology (NIST).

2. Lucifer is the 128-bit encryption algorithm developed by IBM that won the contest organized by the NIST.

3. The National Security Agency (NSA) made a modification to the key size to of Lucifer before adopting it as the official Data Encryption Algorithm (DEA).

Tip	See http://lasecwww.epfl.ch/memo/memo_des.shtml to learn six ways to break DES.

Triple DES

1. Understand the improvements included with 3DES that made it stronger than DES.

Advanced Encryption Standard

1. Rijndael became the Advanced Encryption Standard (AES) after winning another contest organized by the NIST.

International Data Encryption Algorithm

1. Understand the main characteristics of IDEA, including its block size and key size.

Blowfish

1. Understand the main characteristics of Blowfish, including its block size and key size.

Tip	Blowfish source code available at http://www.schneier.com/blowfish-download.html.

RC4

1. Understand the main characteristics of RC4.

RC5

1. Understand the main characteristics of RC5, including its block size and key size.

Asymmetric Algorithms

1. Understand the basics of asymmetric algorithms. Asymmetric algorithms use two keys that are mathematically related, so data encrypted with one key can be decrypted using the other key.

2. Understand the concept of public and private keys and how they can be used to encrypt and decrypt a message with integrity and confidentiality.

3. Understand the advantages and disadvantages of asymmetric algorithms with respect to symmetric algorithms.

RSA

1. RSA is an asymmetric algorithm developed in 1978 by Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman.

2. Understand the mathematical aspects of RSA, including one-way functions and factoring large numbers.

Diffie-Hellman

1. Diffie-Hellman can be used for secure key distribution.

2. Diffie-Hellman does not provide encryption.

Elliptic Curve Cryptography

1. ECC is a perfect candidate for wireless devices and cellular telephones.

ElGamal

1. Understand the main characteristics of Elgamal, another public key algorithm used to encrypt data, create digital signatures, and exchange secret keys.

Tip	Read https://technet.microsoft.com/en-us/library/aa998077(v=exchg.65).aspx for an article on public key cryptography.

Digital Signatures

1. Understand how digital signatures employ asymmetric algorithms to provide message integrity, authenticity and nonrepudiation.

Digital Signature Standard

1. Understand federal government requirements for verifying digital signatures using algorithms, such as RSA and DSA for digital signatures and SHA for computing hash values.

Pretty Good Privacy

1. PGP is a free e-mail encryption program developed by Phil Zimmerman.

2. PGP has evolved into the Internet standard for PGP messages, now called OpenPGP.

Secure Multipurpose Internet Mail Extension

1. Understand the main characteristics of S/MIME.

Sensitive Data Encryption

1. Understand the main characteristics of sensitive data encryption.

Hashing Algorithms

1. Understand the main characteristics of hashing algorithms and how they can be used to provide message integrity.

2. Understand Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1) and the security problems related with the SHA-1 algorithm. Modern systems are upgrading to SHA-2 and SHA-3.

Understanding Public Key Infrastructure (PKI)

1. PKI is not an algorithm; it's a structure consisting of programs, protocols, and security policies for encrypting data and uses public key cryptography to protect data transmitted over the Internet. This section describes the basic aspects of PKI and how it is used in creating certificates.

Components of PKI

1. A certificate is a digital document that verifies that the two parties exchanging data over the Internet are really who they claim to be.
2. Understand the process of issuing a certificate by a CA and how certificates can be used to validate the identity of a party.

Expiring, Revoking, and Suspending Certificates

1. Certificates have expiration dates. Understand the requirements to renew a certificate.
2. Understand the reasons for revoking a certificate and the process of revocation. Certificate Revocation Lists (CRLs) are used to indicate what certificates have been revoked or suspended.
3. Understand the reasons why a certificate can be suspended.

HTTP Strict Transport Security

1. HSTS was created in 2012 as a mechanism for Web servers to tell clients they require secure communications.
2. The two things HSTS does to promote secure client-server communications:
    a. It forces all traffic between a Web browser and a Web server to be sent over a secure channel.
    b. If the Web server's certificate cannot be validated by the browser, the browser will disallow access to the Web site.

Backing Up Keys

1. Backing up keys is a critical process and should be done by a CA.

Microsoft Root CA

1. Understand the steps for configuring a Root CA in Windows Server 2008r. See Figures 12-4 through Figure 12-7

Understanding Cryptography Attacks

1. Understand the difference between an active and passive attack.

Birthday Attack

1. Understand how birthday attacks can be used to find mathematical weakness in hashing algorithms.

Tip	See http://mathworld.wolfram.com/BirthdayProblem.html to solve the birthday problem.

Mathematical Attacks

1. The categories of mathematical attacks:
    a. Ciphertext-only attack
    b. Known plaintext attack
    c. Chosen-plaintext attack
    d. Chosen-ciphertext attack
    e. Side-channel attack
2. Understand the differences between these categories of attacks.

Brute-Force Attack

1. A brute force attack can be used to guess passwords by trying every possible combination of letters.

Man-in-the-Middle Attack

1. Understand the Man-in-the-Middle attack and the complete process for conducting a Man-in-the-Middle attack.

Tip	Read more on the Man-in-the-Middle attack at http://www.tomsguide.com/us/man-in-the-middle-attack,news-17755.html

SSL/TLS Downgrade Attack

1. With a SSL/TLS downgrade attack, an attacker who intercepts the initial communications between a Web server and a Web browser can force a vulnerable server to insecurely renegotiate the encryption being used down to a weaker cipher.

2. The fix for this issue was to make sure all ciphers allowed by a server are secure.

Dictionary Attack

1. Understand a dictionary attack and the legal issues involved in performing such an attack.

Replay Attack

1. A replay attack is a type of attack where the attacker captures data and attempts to resubmit the captured data, so that the device thinks a legitimate connection is in effect.

Understanding Password Cracking

1. Cracking passwords is illegal in the United States.

2. The general steps for cracking passwords:
    a. Obtain the password file from the system
    b. Perform a dictionary attack on the file using automated password cracking programs

3. There are several password cracking programs, including:
    a. Hashcat
    b. John the Ripper
    c. Ophcrack
    d. EXPECT
    e. L0phtcrack
    f. Pwdump7

4. See Figures 12-8 through 12-10 for the password cracking process.

Additional Resources

1. Introduction to Codes, Ciphers, and Codebreaking:
   http://www.vectorsite.net/ttcode_01.html

2. The Legacy of DES:
   http://www.schneier.com/blog/archives/2004/10/the_legacy_of_d.html

3. What is Elgamal Cryptosystem?:
   http://www.x5.net/faqs/crypto/q29.html

4. Why Textbook ElGamal and RSA Encryption are Insecure:
   http://crypto.stanford.edu/~dabo/abstracts/ElGamalattack.html

5. Using the Windows Certificate Viewer:
   http://www.dartmouth.edu/~deploypki/materials/modules/using/certstores/windows.htm

Key Terms

- **Advanced Encryption Standard (AES)**
- **asymmetric algorithm**
- **authentication**
- **birthday attacks**
- **block cipher**
- **Blowfish**
- **brute-force attack**
- **certificate**
- **certification authority**
- **cipher**
- **ciphertext**
- **cryptanalysis**
- **cryptosystem**
- **data at rest**
- **Data Encryption Algorithm (DEA)**
- **Data Encryption Standard (DES)**
- **dictionary attack**
- **digital signature**
- **encryption algorithm**
- **hashing algorithm**
- **HTTP Strict Transport Security (HSTS)**
- **International Data Encryption Algorithm (IDEA)**
- **key**
- **keyspace**
- **man-in-the-middle attack**
- **mathematical attack**
- **message digest**
- **Message Digest 5 (MD5)**
- **nonrepudiation**
- **OpenPGP**
- **plaintext**

- **Pretty Good Privacy (PGP)**
- **private key**
- **public key**
- **public key cryptography**
- **public key infrastructure (PKI)**
- **rainbow table**
- **RC4**
- **RC5**
- **replay attack**
- **salt**
- **Secure Hash Algorithm 1 (SHA-1)**
- **Secure Multipurpose Internet Mail Extension (S/MIME)**
- **SSL/TLS downgrade attack**
- **steganography**
- **stream cipher**
- **substitution cipher**
- **symmetric algorithm**
- **Triple Data Encryption Standard (3DES)**