Principles of Cyber Security: Lecture 06- The components of cryptographic system

Contents

Lecture 06: The components of cryptographic system

Outline

- Overview
- Objectives
- Quick Quizzes
- Class Discussion Topics
- Additional Resources

Principles of Cyber Security: Lecture 06- The components of cryptographic system

Lecture Notes

Overview

In this lecture, you will learn practical methods for applying cryptography to protect data.

Lecture Objectives

6.1 Define cryptography.

6.2 Describe limitations of cryptography.

6.3 List the various ways in which cryptography is used.

Principles of Cyber Security: Lecture 06- The components of cryptographic system

OB.6.1: Define cryptography

6.1.1 Implementing Cryptography

1. The cryptography is improperly applied can lead to vulnerabilities that threat actors will exploit.
2. Implementing cryptography includes understanding:
    a. Key strength
    b. Secret algorithms
    c. Block cipher modes of operation
    d. Cryptographic service providers
    e. The use of algorithm input values

Key Strength

1. The three primary characteristics that determine the resiliency of the key to attacks (key strength):
    a. Randomness
    b. Length
    c. Cryptoperiod
2. Use Table 4-1 in your discussion of key strength.

Secret Algorithms

1. Discuss why it is not effective to keep algorithms secret:

a. For cryptography to be useful it needs to be widespread

Block Cipher Modes of Operation

1. Explain that a block cipher mode of operation specifies how block ciphers should handle blocks of plaintext.
2. Discuss some of the common modes:
    a. Electronic Code Book (ECB)
    b. Cipher Block Chaining (CBC)
    c. Counter (CTR)
    d. Galois/Counter (GCM)

Crypto Service Providers

1. The crypto service provider allows an application to implement an encryption algorithm for execution.
2. The crypto service providers :
    a. Implement cryptographic algorithms
    b. Generate keys
    c. Provide key storage
    d. Authenticate users by calling various crypto modules to perform specific tasks

Algorithm Input Values

1. Salt is a value that can be used to ensure that plaintext, when hashed, will not consistently result in the same digest. Mention that a randomized salt will give added protection.
2. Nonce as an input value that must be unique within some specified scope.
3. Initialization vector (IV) is the most widely used algorithm input.
4. IV may be considered as a nonce with an additional requirement: it must be selected in a non-predictable way.

Principles of Cyber Security: Lecture 06- The components of cryptographic system

Quick Quiz 1

1. Which of the following is NOT one of the characteristics that determine the resiliency of a key to attacks?
    - randomness
    - cryptoperiod
    - unique
    - length

2. Which block cipher mode of operation methods encrypts plaintext and computes a message authentication code (MAC) to ensure that the message was created by the sender?

    a. Electronic Code Block (ECB)

    b. Cipher Block Chaining (CBC)

    c. Counter (CTR)

    d. Galois/Counter (GCM)

3. Which of the following terms best describes a publicly accessible centralized directory of digital certificates that can be used to view the status of a digital certificate?
   a. Certificate Signing Request (CSR)
   b. Certificate Revocation (CR)
   c. Certificate Repository (CR)
   d. Online Certificate Status Protocol (OCSP)

4. Revoked digital certificates are listed in a(n) ____, which can be accessed to check the certificate status of other users.

5. The beginning point of the chain is known as which of the following?
   a. root digital certificate
   b. user digital certificate
   c. master digital certificate
   d. server digital certificate

OB.6.2: Describe limitations of cryptography.

6.2.1 The limitations of cryptography

While cryptography is a crucial tool for securing information and communication, it has its limitations. Here are some key limitations of cryptography:

- **Key Management:**
  - Cryptography relies heavily on the use of keys for encryption and decryption. The secure management of keys is challenging, especially as the number of keys increases. Key distribution, storage, and protection become critical issues.
  -
- **Key Exchange:**
  - The secure exchange of cryptographic keys between parties is a potential vulnerability. If a third party intercepts or compromises the key exchange process, it may undermine the security of the encrypted communication.

- **Algorithm Vulnerabilities:**
  - The security of cryptographic systems depends on the strength of the underlying algorithms. If a cryptographic algorithm is found to have vulnerabilities or is broken, it can compromise the security of the entire system.

- **Quantum Computing Threat:**
  - The emergence of powerful quantum computers poses a potential threat to traditional cryptographic algorithms. Quantum computers have the potential to break widely used encryption schemes, such as RSA and ECC, which are currently considered secure against classical computers.

- **Implementation Flaws:**
  - Poorly implemented cryptographic systems can introduce vulnerabilities. Flaws in the software or hardware implementations may create avenues for attackers to exploit weaknesses and bypass encryption.

- **Cryptographic Backdoors:**
  - There have been concerns about the possibility of intentional or unintentional backdoors being built into cryptographic systems. These backdoors could be exploited by malicious actors or abused by governments for surveillance purposes.

- **Brute Force Attacks:**
  - Cryptographic systems can be susceptible to brute force attacks, where an attacker systematically tries all possible keys until the correct one is found. The security of a system depends on the length and complexity of the key, making longer keys more resistant but also more resource-intensive.

- **Side-Channel Attacks:**
  - Side-channel attacks exploit information leaked during the execution of cryptographic algorithms, such as timing information, power consumption, or electromagnetic radiation. These attacks can potentially reveal the secret key.

- **Human Factor:**
  - Human factors, such as weak password choices, poor key management practices, or the sharing of sensitive information, can undermine the effectiveness of cryptographic measures. Education and awareness are crucial to mitigating these risks.

- **Evolution of Threats:**
  - As technology evolves, so do attack techniques. New threats and attack methods may emerge that were not anticipated when cryptographic systems were initially designed, potentially rendering some encryption methods obsolete.

OB.6.3: The various ways in which cryptography is used:

6.3.1 Key Ways in Which Cryptography is Used

- **Secure Communication:**
  - **Encryption of Messages:** Cryptography is used to encrypt messages, ensuring that only authorized parties can decipher and understand the content.

- **Data Integrity:**
  - **Hash Functions:** Cryptographic hash functions are employed to verify the integrity of data. Any change in the data will result in a different hash value, alerting users to potential tampering.

- **User Authentication:**
  - **Password Protection:** Cryptography helps secure user passwords through techniques like hashing and salting, preventing unauthorized access to accounts.

- **Digital Signatures:**
  - Authentication of Documents: Cryptographic digital signatures provide a way to verify the authenticity and origin of digital documents, assuring that they have not been altered.

Principles of Cyber Security: Lecture 06- The components of cryptographic system

- **Virtual Private Networks (VPNs):**
  - Tunneling and Encryption: Cryptography secures data transmitted over VPNs, ensuring the confidentiality and integrity of information transferred between connected devices.

- **Secure File Storage:**
  - File Encryption: Cryptography is used to encrypt files or entire storage systems, protecting sensitive information from unauthorized access.

- **Email Security:**
  - Pretty Good Privacy (PGP): PGP employs cryptographic techniques to secure email communications, providing confidentiality, authentication, and integrity for messages.

- **Mobile Device Security:**
  - Device Encryption: Cryptography is used to encrypt data stored on mobile devices, protecting it from unauthorized access in case of loss or theft.

- **Cloud Security:**
  - Data Encryption in Transit and at Rest: Cryptography secures data both in transit to and from the cloud and when stored on cloud servers.

- **IoT Security:**
  - Device Authentication and Communication Security: Cryptography is used to secure communication and authenticate devices in the Internet of Things (IoT) ecosystem.

Class Discussion Topics

1. Discuss the core concepts of cryptography, such as encryption, decryption, and key management.
2. Discuss the limitations inherent in cryptographic algorithms, including vulnerabilities that may be exploited by advancements in mathematics or computing power.

Additional Projects

1. Ask your students to read the following article about the risks of key recovery, key escrow, and trusted third party encryption at **https://www.schneier.com/paper-key-escrow.html** and write a report summarizing its most important points.

2. Ask your students to read more about SSL and TLS and write a report explaining how they work. Use the following link as a starting point: **http://computer.howstuffworks.com/encryption4.htm** .

Additional Resources

1. S/MIME

   https://www.justinrummel.com/what-is-smime-email-and-why-should-i-be-using-it/

2. Introduction to Cryptography

   https://users.ece.cmu.edu/~adrian/630-f04/PGP-intro.html

3. RFC2516 - A Method for Transmitting PPP Over Ethernet (PPPoE)

   http://www.faqs.org/rfcs/rfc2516.html

4. Digital certificate

   https://support.office.com/en-us/article/Digital-signatures-and-certificates-8186CD15-E7AC-4A16-8597-22BD163E8E96

5. IP Encapsulating Security Payload (ESP)

   http://www.ietf.org/rfc/rfc2406.txt