Introduction to Information Security

—— Review

Dr. Tianlei HU

Associate Professor

College of Computer Science, Zhejiang Univ.

htl@zju.edu.cn

Review of Concepts

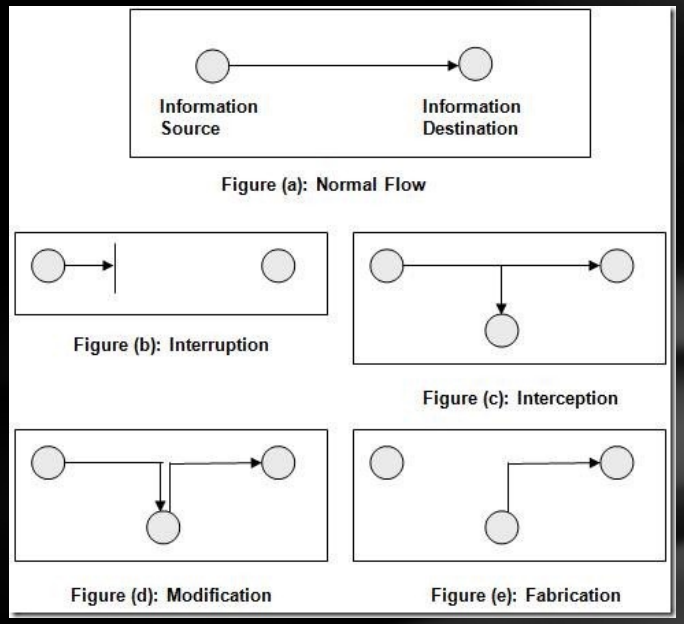
- Computer Security
- Cryptography
- Authorization and Access Control
- Network Security

Concepts of Computer Security

- Kerckhoffs Principle
  - "A cryptosystem should be secure even if everything about the system, except the key, is public knowledge."—— was stated by Auguste Kerckhoffs in 1883
  - 增强安全性：**凡是难于改变且长时间使用的东西都只能假设对手会知道**
    - 没有理由认为**加密算法本身具有好的保密性**。
    - **安全依赖于密钥的保密而不依赖于算法的保密**，密码的强度必须在对手已知算法的前提下定义。
- 3(~4) elements of computer security
  - **Confidentiality**—— can others see your data?
  - **Integrity**—— can your data be illegally changed?
  - **Availability**—— will the resource be accessible?
  - **Authenticity**—— proof of identity
- Concepts of Computer Security： Asset, Threat, Vulnerabilities, Risk
  - Asset (资产) – People, property, and information.
  - Threat (威胁) – Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.
  - Vulnerability (漏洞) – Weaknesses or gaps in a security program that threats can exploit to gain unauthorized access to an asset.
  - Risk (风险) – The potential for an asset's loss, damage, or destruction due to a threat exploiting a vulnerability.

Concepts of Computer Security

- Ways of security attacks: Interruption, Interception, Modification and Fabrication



- Passive Attacks & Active Attacks :
  - Passive Attacks : Interception
    - Difficult to detect —— Prevention is more effective than detection.
  - Active Attacks : Interruption, Modification and Fabrication
    - Easy to detect, difficult to prevent, can be resume from damage

Concepts of Cryptography(1)

- Fundamentals of Cryptography： plaintext, ciphertext, encryption algorithm, the decryption algorithm
  - plaintext， P
  - ciphertext， C
  - encryption method， E()
  - decryption method， D()
  - key， K
  - $C = E_K(P)$
  - $P = D_K(C)$
- Principle of Classical Cipher & Crack
  - Caesar's Cipher, Queen Mary's Cipher, Vigenere Square, Book Cipher
  - Frequency analysis， the Kasiski Test
  - Enigma principle
- Symmetric Key Cryptography
  - Fundamentals
  - Fiestel structure
  - Fundamentals and Structure of DES / 3DES / AES

Concepts of Cryptography(2)

- Asymmetric Key Cryptography
  - Fundamentals
  - What is the difference between Symmetric and Asymmetric Key Cryptography?
    - 公开密钥加密算法依赖于数学函数而不依赖于替代和置换
    - 公开密钥加密算法是非对称的，使用两个独立的密钥，因此又称“非对称加密算法”
    - 公钥密码使得发送端和接收端在不共享任何秘密消息（密钥）的前提下即可交换大量秘密信息（实现保密通信）成为可能！
  - Functions： encryption, signature, key exchange
  - The One-Way functions
    - DH Algorithm： **计算大整数的整数次幂比较容易，但计算离散对数很困难**
    - RSA Algorithm： **大素数相乘很容易，但大合数质因子分解很困难**

Concepts of Cryptography(3)

Pros/Cons of Symmetric / Asymmetric Key Cryptography & Application Model:

- Symmetric key :
  - Pros: Cheap, fast
    - cheap integrated circuit chips can be used for encryption and decryption.
  - Cons: Key distribution is a problem!!
- Public key:
  - Pros: Key distribution is no longer a problem!
  - Cons: Relatively expensive and slow
    - the encryption/decryption hardware IC chip is extremely expensive
- In application:
  - Use Public Key Cryptography (such as RSA) to distribute keys;
  - Use Symmetric Key Cryptography (such as DES) for encryption and decryption

Concepts of Cryptography(4)

- The demand for digital signature
  - "Bind" to the signed document
  - The recipient can verify the signature, and anyone else can not forge signatures.
  - The signer can not deny their signature.
  - The signatures must be confirmed by a third party so that it can resolve disputes.
  - Able to verify the signature of the date and time of the signature, the signature moment of the content of the message (not reusable, can not be forged, and can not be changed, time-binding)
  - Why does the digital signature use a one-way hash function
- Concepts of the one-way hash function
- Concepts of MAC, the Message Authentication Code

Concepts of Authentication and Authorization(1)

- Implementation of Authentication:
  - What do you have?: ID card, passport, key, smart card, USB card, mobile phone
  - What do you know?: password, birthday, ID number, the answer to a question
  - Where are you?: IP address
  - Personal characteristics (what are you?):
    - Biometrics characteristics: fingerprint, palm print, iris, facial contours, DNA, etc.
    - Behavioral characteristics: handwriting, vocal print, stoke, walking, etc.
- Storage, choice, and protection of password:
  - Concepts of a Dictionary Attack and Salt Cipher
  - How to choose and protect our password?

Concepts of Authentication and Authorization(2)

- **Concepts of Secure Access Control/Authorization**
  - Three elements of access control：
    - Subject： An entity that can access objects, such as user or application process, etc
    - Object ： The object being accessed, such as files, programs, data, etc
    - Privilege： The subject can use the object's methods, such as read, write , delete, execute, sublicense, etc
- Concepts and principles of DAC, MAC, and RBAC
  - Concepts of Bell-Lapadula principle (in MAC)
  - Covert Channel (in MAC)
  - Role(in RBAC)
- The core principle of Secure Access Control
  - The smallest privilege, separation of powers
  - Authorized management model

Concepts of Network Security

- Common attacks:
  - Sniffing, ARP Spoofing, IP Spoofing
  - TCP SYN Flooding (Important!)
    - Concepts, how to attack, why it can succeed, and how to prevent.
  - TCP SYN prediction、TCP Congestion Control
  - DNS Spoofing
- Concepts of IPSEC
  - Authentication Headers(AH)、Encapsulating Security Payloads(ESP)、Security Associations(SA)、Model: transport mode and tunnel model
- Concepts of TLS/SSL
  - SSL connection and SSL session、SSL/TLS protocol
- Malicious Code:
  - Concepts and differences of virus, worm, and Trojan horse.
  - Defenses of Malicious Code
  - How are botnets formed, and how is it used for attack? Concepts of DDOS attack

The Exam

日期: 2023.4.23（下下周日）

时间: 8:00-10:00

地点: **紫金港东2-104**

闭卷考试，不允许携带任何书籍和电子设备。

英文试卷，可用中英文答题。

题型：填空、单选、判断、问答、应用。