Chapter 1Concepts and Base of Information Security

2017年3月3日 13:26

BY LSY

- History of info security and evolution
  - The earliest info security?
  - The Landmark event of four evolution of computer security?
- Significance and properties of computer security
  - What’s special of computer security?
- Concepts, attack and confront of computer security
  - Three elements of computer security
  - Concepts of computer security: vulnerabilities, threats, attacks, control
  - Ways of computer attack and its classifier
  - Security system, security services, security mechanisms, operational and human issues

1. Outlines:
   - History and Evolution of Information Security
   - Objectives and Properties of Information Security
   - Concepts of Computer Security, Attack and Anti-Attack

2. 加密方法
   - 替代加密：将一个信息用一个符号去替代
   - 位移加密：
   - 豪密：
   - 凯撒密码：最早的密码，将字母都后移3位
   - 棍子密码 Scytale Cipher：

3.Information Hiding/Steganography
隐写术

4.The evolution of Cryptography(密码学)
   - The Kerckhoffs’ Principle
     - 从经验->科学，依赖密钥
   - Computers
     - 加速enctryption&decryption,cryptography evolved from Manual to Mechanical and Electronic
   - Public Key Ciphers 公钥密码学
     - Make it possible to exchange large amount of secret message without sharing any secret key between the sender and receiver
     - RSA加密算法——非对称加密算法：对极大整数做引述分解
   - Internet
     - 区块链，去中心化

5.Computer Security
   - PC Era： Virus ravages——show off/destroy
   - Internet Era：Hacker, worm and DOS burst out——benefit&monetize

- [x] 2017/3/6 10:03

6. Distinctness of computer based information security & paper based information security：
   - Can't distinguish between the original and the copy;
   - Alteration on digital paper will leave nothing;
   - Digital documents are really easy to delete;
   - Digital Information only depends on binary information;

7. Chatacteristics of computer security

- Comprehensiveness
  - System Security depends on the weakest link
- Procedural
  - It’s a constant back and forth rising spiral security model
- Dynamic
  - The entire security system is in the process of constantly update, improve and progress
- Hierarchy
  - Have to use multi-level security technologies, method and ways to resolve security risk
- Relativity
  - Security is relative, and no absolute security

Concepts of Computer Security

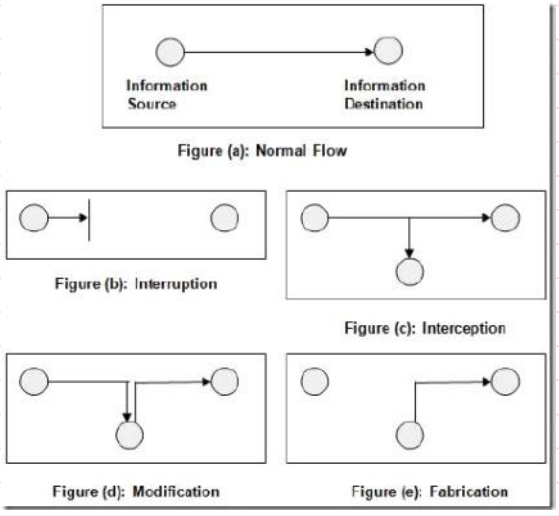
8. 3 elements of computer security:

- Confidentiality 保密性
- Integrity 完整性
- Availability 可用性
- Authenticity 真实性

9. Concepts of computer security

- Vulnerabilities / 漏洞
  - Is a weakness in the security system
- Threats / 威胁
  - Is set of circumstances that has the potential to cause loss of harm
- Attacks / 攻击
  - A human or another system can exploit vulnerabilities to initiates an attack
- Control / 控制、对抗措施
  - Is an action, device, procedure, or technique that removes or reduces the vulnerabilities

10. Types of security threat



- Interruption : availability
- Interception 信息泄露: Confidentiality
- Modification : Integrity
- Fabrication : Authenticity

- Passive Attack 被动攻击——prevention
  - Interception

- Active Attack 主动攻击——detect+restore
  - 后三者

11.The Goal

- Prevention
- Detection
- Recovery

12. Against security threats

- Authentication
  - Make sure that the entities of communication is the actual claimed entities, include peer

entity authentication and data origin authentication.

- Access control
  - Prevent the unauthorized visit to resource
- Data Confidentiality
  - Prevent data leakage, include linked confidentiality, unlinked confidentiality, selected fiel
  - confidentiality and flow confidentiality.
- Data Integrity
  - Make sure the received data is sent from authorized entity, and without modification, insert,

delete and replay.

- Non-Repudiation
  - Prevent repudiation in communication from any entity
- Availability
  - Make sure the availability of service