Introduction.

1. Three Main Requirements.
2. OSI Security system: 5 service, 8 mechanism.
3. Type of Attack.

Cryptography

一、Symmetric key Cryptography.

1. Substitution Cipher: Caeser Cipher.
2. Block Ciphers
   (1) Basic Techniques: Substitution, Permutation.
   → S-P Network (SPN): boxes.
   (2) Goal: Confusion, Diffusion.
   (3) Data Encrption Standard. (DES) (3DES)
   Advanced Encrption Standard. (AES)
3. Stream Ciphers
   (1) Work Pattern: bit by bit, pseudo raaclom
   (2) Structure.
   (3) RC4.
4. Cipher Modes.

二、Public key Cryptography.

1. Goal: key Distribution, Digital Signature.
2. Characteristics.
3. RSA

三、Hash Functions

二、 Hash Functions.
1. Concept: compression.
2. Functions: MD5. SHA-1.
3. Birthday Attacks.
4. Application: MAC, Digital Signature.

四. Random Numbers.
1. True, Pseudo.
2. Strength.

五. Digital Signature.
1. Structure
2. RSA based Digital Signature.

六. Message Authentication Code.
1. Shared-key based MAC.
2. HMAC.

Authentication.
一、UsrName-Password (Shared key: pwd).
1. encryption / de
2. hash
3. in table.

二、Challenge-Response Authentication Mechanism. (shared-key).

1. Process
2. Ways: encrypher, hash, two way.
3. Replay Attack.

三、Key Distribution Center based Authentication.
1. Structure
2. Replay Attack.

四、Public Key Cryptography based Authentication.
1. Structure: Directory.

五、Single Sign On.
1. Kerberos.
2. Open ID.

Authorization

一、Access Control structure.
1. Elements
2. Access Control Matrix.
3. Access Control Lists, Capabilities.
4. Role-based Access Control.
(1) Structure
5. Security Labels and Partial Ordering.
(1) < Upper Bound, Lower Bound, Lattice

(1) ≤, upper bounds, lower bounds, Lattices.

(2) System High, Sys Low.

三. Access Control Models and Policies.

1. Information Flow Policies.
   (1) Labels
   (2) Read / write Access. Control.
   (3) Three Elements.

2. Integrity and Transaction.

3. Multi-Level Security.
   (1) Confidentially Policies: BLP model.
      ① levels.
      ② Read up/down, Write up/down.
      ③ no read up.

   (2) Integrity Security: Biba model.
      ① levels.
      ② no wirite up.

4. Chinese Wall Model.

* Salted pwd.
* 数字证书.

* pKa.

* pH.