Chapter 15 - Security

> Key security enable: **Encryption**

1. Security Problem

1.1. Security Violations

There are 2 types of security violations: by **intention** (malicious) or by **accident**.

1.2. Forms of misuse

And there are several forms of accidental or malicious misues:

- Breach of **Confidentiality**: unauthorized reading of data.
- Breach of **Integrity**: unauthorized modification of data.

- Breach of **Availability**: unauthorized destruction of data by causing havoc or defacement.
- **Theft of Service**: unauthorized use of resource.
- **Denial of Service**: preventing legitimate use of service.

1.3. Attacking Methods

- **Masquarading**: pretend to be s/o
- **Replay Attack**: keep system busy by repeat of valid data transmission.
- **Message Modification**
- **Man in the middle attack**
- **Session Hijacking**: MITM + intercepting an active session.

1.4. Program Threats

- **Trojan House**: code segment misuses its env, login emulation, spyware. Attached to a program, but does not replicate.
- **Trap Door**: leaving secret access point, backdoor
- **Logic Bomb**: initiates a security incident under certain conditions.
- **Stack and Buffer Overflow**: overload the data until return address is modified. Solution: SPARC and Solaris throws exception when exec from stack memory, Linux and Windows XP mark those page as non-exec.
- **Virus**: attach itself to a program, self replicate & infect other program. Specific to CPU arch, OS, apps. **Why Windows has more virus?** Linux/UNIX has separated users/roots, where as Windows users usually have admin privilege, and Windows systems outnumber UNIX/LINUS. Categories of virus: Macros, File, Boot sector, Source Code, Polymorphic, Encrypted, Stealth, Tunneling, Multipartite, Armored.
- **Worm**: replicate functional copies of themselves but as separate entities.

2. Cryptography as Security Tool

There are 2 types of encryption algorithms:

2.1. Symmetric Encryption

- Mostly base on **Transformation**.
- **DES: Most commonly** used **symmetric block-encryption** algorithm. 64-bit chunk value and 56-bit key. XORED previous ciphertext before encrypt.
- **Triple DES**: improve version of DES with 3 times encryption using 2 or 3 keys.
- **AES** (Advanced Encryption Standard): key length 128, 192, 256, and data chunk of 128-bit.
- **Twofish**: variable key up to 256-bit, 128-bit chuk value.
- **RC4**: **Stream Cipher**, when length of comm makes block cipher slow. Used in WEP, HTTPS.

2.2. Asymmetric Encryption

- **Key difference with symmetric**: the enc and dec keys are different.
- Mostly base on **Maths Function**, not Transformations.
- **Not for large amount** of data.
- Used for small amount of data, authentication, confidentiality, key distribution.
- **RSA**: block-cipher public key algo.
    - Encryption algo is $E(k_e, N)(m) = m_e^k modN$, where k_e satisfies $k_e k_d mod(p-1)(q-1) = 1$; decryption is $D(k_d, N)(c) = c_d^k modN$

2.3. Authentication

- **Authentication** is used to verify a msg or doc was authored by a certain party, and not altered or modified, i.e. integrity verification.
    - Each msg has an authenticator (generated by the sender) and will be verified by the receiver.
    - There are 2 types of auth algos: MAC (symm enc) and Digital Signature (asym enc, key is inversed).
    - Fewer computations, auth is shorter than msg, for non-repudiation.
- **Key Distribution**: use CA to prove who owns the public key.
- **Application**: SSL, HTTPS, IPSEC/VPN

2.4. User Authentication

- Use password, symmetric, asymmetric enc, user identity (key, card, attribute, fingerprint, retina, etc)
- **One Time password**: uses SecurID, S/K system.

3. Security Defense

- 2 types: Intrusion Detection (IDS), and Intrusion Prevention (IPS).
- **Intrusion**: signature-based detection of dangerous behavior patterns (need benchmark of normal behavior first, requires upgrade of signatures), anomaly detection.
- False Alarm = False Positive (must be low), Missed Intrusions = False Negtive.
- Network firewall: DMZ - semitrusted domain.

3.1. Security Classification

Base on US Department of Defense: D(minimal security), C(some protection), B(C+sensitivity labels), A(formal design, verification techniques).

4. Questions

4.1. Which symmetric encryption algorithm has longest key length?

Ans: RC5 (0-2040 bit)

4.2. Differences of Asymmetric and Symmetric Encryption?

4.3. How many bit do MD5 & SHA1 produce?

4.4. How many types of Authentication Algorithm?

4.5. Why false alarm must be low in IDS & IPS?