Information Security : Attacks and Defense Mechanisms

KR Chowdhary, Professor & Head

Email: kr.chowdhary@gmail.com

Department of Computer Science and Engineering
MBM Engineering College, Jodhpur

Objective

In order to build a secure system, designers must first decide exactly what “secure”means for their particular need. In a private company secrecy may be related to nondisclosure of confidential accounting data or trade secrets, or to the enforcements of privacy regulations regarding personal, medical, or credit records.

Security services

Information and network security risks are increasing with the growth of the number of threats and sophisticated attacks.

- A user U_A, transmits a file to U_B. User U_H (not authorized to access the file) captures a copy of the file during transmission.
- A network manager Man_D, transmits a message to a networked computer Com_E to grant accesses / authorizations for new users. U_H intercepts the message, alters it and forwards to Com_E.
- A message sent from customer U_A to stockbrocker U_B to execute some transactions. U_H intercepts and sends several copies.
- An employee Y is terminated. The personal manager sends message to server to invalidate $Y's$ account. Y delays the message, and retrieves the sensitive information before message reaches.

Aspects of security needs

Need of a systematic way of defining the requirements for security and characterizing the approaches to satisfy the requirements.

- Identify Security attacks
- Identify Security mechanisms
- Identify Security services

Security Services

- Authentication
- Confidentiality
- Integrity
- Non-repudiation
- Access-control
- Denial of Service (availability Function)
- Spoofing

Common Attacks and Defense Mechanisms

- Eavesdropping
- Interception may be caused due to eaves dropping
- Cryptoanalysis
- Password Pilfering
  1. Guessing
  2. Social Engineering
  3. Phising (Mass social engineering attacks, , the main form are disguised emails, as if these emails were sent by banks, credit card holders, etc. In reply we supply the information, which go to wrong hands.)
  4. Dictionary attacks
  5. Password Sniffing: These are programs, which capture remote login information such as user names and user passwords.
- Password Protection.
  1. Use long passwords with combinations
  2. Do not reveal password to any one
  3. Change password periodically

Common Attacks and Defense Mechanisms

- Password Protection.
  1. Do not use same password for different accounts
  2. Do not use remote logins
  3. Avoid entering any information in any popup window
- User authentication methods:
  1. Using passwords
  2. biometrics,
  3. Electronic passes authenticated by the issuer.
- Identity Spoofing: Allows attackers to impersonate a victim without using the victim's passwords. Following are common attacks:
  1. man-in-the-middle attacks

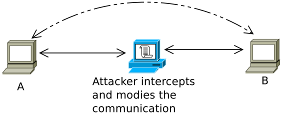

Figure: Man-in-the-middle attacks.

Common Attacks and Defense Mechanisms

- Identity Spoofing:
  1. Message Replays:
     Common mechanisms to thwarting message replay attacks:
  2. Attach a random number to the message
  3. Attach a time stamp to the message
  4. Use nonce and time stamp together
- Network Spoofing: IP spoofing is one of the major network spoofing technique. Following are the types:
  1. Syn Flooding: Exploits the implementation side effect of the TCP/IP network protocol.
  2. TCP hijacking:
  3. ARP Spoofing:
- Buffer overflow Exploitation

```
int main(){ char buffer[8];
    char *str = "This is a test of buffer overflow.";
    strcpy(buffer, str);
    printf("%d", buffer); }
```