Man-in-the-middle Attack

A man-in-the-middle attack often refers to an attack in which an attacker secretly intercepts the electronic messages going between the sender and the receiver and then capture, insert and modify messages during message transmission.

Attack Methods

If sender transmits messages without appropriate encryption and digital signature, the attacker may exploit the vulnerabilities in the network to capture and modify the messages, and send the modified messages to the receiver. Because the network transmission still works properly, both the sender and receiver will find it difficult to notice that the messages have already been trapped, intercepted or tampered by an intruder. Since this type of attack may neither involve installation of malicious code such as computer virus or Trojan horse nor leave any logs on user's computer, it is therefore difficult to discover it by using anti-malicious code software such as anti-virus software.

Potential Threats

What are the potential threats you will face when you are under man-in-the-middle attack?

If a computer user performs online transactions without using encryption, the man in the middle may capture the user's bank account number and password from the transmitted messages and log into the account to steal money or to perform other illegal activities, leading to the user's financial loss.

If an intruder successfully steals the login ID and password of an organisation's information system, it may be possible for the intruder to steal the organisation's internal sensitive information such as personal information of customers and lead to data leakage.

General Security Precautions

In order to effectively prevent man-in-the-middle attack, you must take good security precautions.

For organisations:

- Use encrypted connections such as HTTPS, SSH, SFTP etc, to encrypt the messages transmitted through the network. As a result, the intruder cannot read or modify the information even if he can intercept the encrypted messages during transmission.
- Use mutual authentication. Since the user must be authenticated by the server and the server also needs to be authenticated by the user, man-in-the-middle attack could be blocked.

For Individuals:

- Configure and enable the encryption features such as WPA with AES encryption for Wi-Fi communication.
- Do not conduct online transactions or use online banking services from cyber cafes or other public terminals.

In addition to the use of data encryption, digital signature and aforementioned security precautions, other related information security measures should also not be neglected.

To learn more about information security, please visit the InfoSec website at: http://www.infosec.gov.hk