Eavesdropping

Eavesdropping

Eavesdropping refers to the unauthorised monitoring of other people's communications. It can be conducted on ordinary telephone systems, emails, instant messaging or other Internet services. Since eavesdropping activities do not affect the normal operation of network transmission, both the sender and the recipient can hardly notice that the data has been stolen, intercepted or defaced.

As the Internet has become more popular, people make use of all kinds of Internet services, for example, emails, chat rooms and social networking websites for communication. If we do not take appropriate security measures when using these communication tools, the risk of being eavesdropped will increase.

Eavesdropping Methods

Eavesdropping usually happens in the following ways:

- Take email as an example. If the sender has not encrypted the email message and has not used digital signature, the attacker can exploit security loopholes on the network to launch a Man-in-the-Middle attack. He may intercept and deface the message before sending it to the recipient, who will be deceived into believing the defaced message and provide personal or sensitive information.
- Generally, data is transferred on the Internet by Hypertext Transfer Protocol （HTTP） standard. Using HTTP standard to transmit personal or sensitive information is comparatively insecure because encryption is not applied to the online transactions and attackers will be able to read sensitive information from the transmitted messages.

Security Measures

Following are the security measures against eavesdropping in Internet communications:

- Use encrypted connection, e.g. Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) which offer better security, to encrypt the data transmitted on the Internet. Even if attackers can intercept the data, they cannot read or deface the information easily.

- Install personal firewall on computers connected to the Internet. Update antivirus software with the latest virus signature or malicious code definition.

- When using public Internet facilities, avoid conducting online transactions or using online banking services.

- Install intrusion prevention system on the computer network of your organisation to detect and prevent further attacks by eavesdroppers.

- Use Internet services with mutual authentication such as Public Key Infrastructure (PKI). A transaction will only be processed after the user's computer has been authenticated by the organisation's server and vice versa. With confirmation of the identities of both parties, the risk of Man-in-the-Middle attacks can be reduced.

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