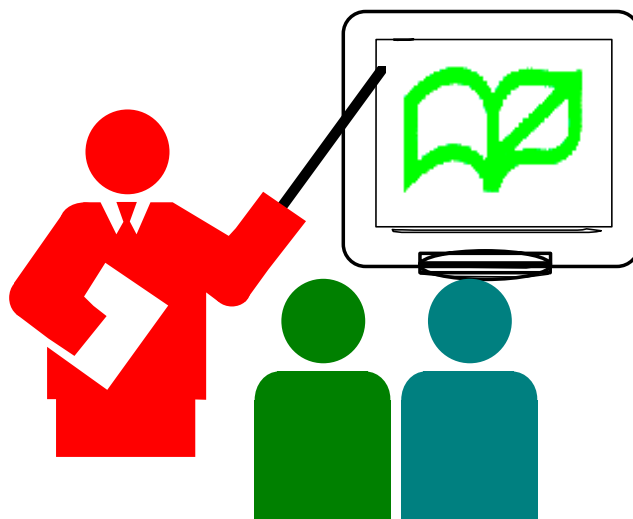


Information Technology in Education Project

Wireless LAN Security

(RM12/2002)



**Infrastructure Division
Education Department
The Government of HKSAR
www.ited.ed.gov.hk**

December 2002

For enquiry on this document, please direct to inspector of Regional Support Section, Infrastructure Division, Education Department at (852) 3123 8108 or write to Principal Inspector, Regional Support Section, Infrastructure Division, 5th Floor, Kai Tak Government Building, 5 Arrivals Road, Kowloon City, Hong Kong.

The full text of this publication is available at the Information Technology Education Resource Centre home page at <http://www.ited.ed.gov.hk>

Wireless LAN Security

Wireless Local Area Network (WLAN) application is becoming more popular in schools. The WLAN technology allows schools to extend their existing network with greater flexibility and more convenience. While enjoying the benefits from WLAN technology, schools themselves should also aware the issues and workarounds of WLAN security.

About this document:

*This paper covers security issues in using WLAN in schools. Basic knowledge of WLAN is required in understanding this paper. WLAN security measures are introduced to enable schools to have a better understanding of the protection of their WLAN system. The main focus of the paper will be based on the **802.11b** technology. However, most of the information is applicable to other WLAN standards.*

Security is a main concern when implementing and managing a network, especially a wireless network. In a wireless network, communication is broadcasted over radio wave. Hence, WLAN is more vulnerable to hackers' attacks or eavesdropping. Schools should take proactive steps to minimize security risks in WLAN.

Security threats of WLAN

In general, hackers are easier to get into a WLAN than a wired network. They can access your network without your permission or notice by placing WLAN devices (either access point or WLAN client) in your network. This is referred to **Insertion**.

(1) Insertion of *wireless client*, such as notebook computer or PDA, to a WLAN access point is easy. Such insertion can be performed remotely within the range of your WLAN coverage, with some of the WLAN information (e.g. SSID) has been known. The hacker can use computers to mimic the legitimate users.

(2) Insertion of unauthorized *WLAN access point* may also happen in a network. However, hackers have to place the access point(s) in the network first. In some instances, a school staff may plug his/her own WLAN access

points into the school LAN for convenience... In that way, he/she may have already opened a backdoor for hackers.

As the signal of WLAN is broadcasting in air, interception and monitoring of the radio signal (**eavesdropping**) are commonly used. If an access point is connected to a hub instead of a switch, all traffic, including the wired traffic, across the hub can be potentially broadcasted over the wireless network. It would be easier for eavesdropping to take place.

Common attacks on WLAN

Here are the common attacks on wireless network which may work within range of your wireless signal. These attacks are usually based on insertion or eavesdropping of wireless access points/clients. In fact, the attacks are common in wired network also.

Wireless Sniffer

By using sniffer software in a wireless client, a hacker can sniff and capture any legitimate traffic. No attack is made during sniffing. The hacker is collecting vital packet information for later attack.

Session Hijacking

If sniffing is possible, it is also possible for a hacker to inject false traffic into a connection. As such, the hacker may be able to issue commands on behalf of a legitimate user by injecting traffic and so hijacking their victim's session.

Spoofing

The hacker uses a mobile device with spoofed MAC (Media Access Control) address. Using packet-capturing software, the MAC address can be found.

Denial Of Service (DOS)

DOS is a common attack for all networks. In a WLAN, the hacker might not steal any

information. The hacker may send continuous data packets to jam the access point, or use a high power radio signal generator to interfere the WLAN clients to access the WLAN. The users at that time cannot access the network service as the network is being kept busy by DOS attack.

Man-in-the-middle attacks

The hacker may set up an access point nearby with a different radio channel. When a user associates with this access point, the username and password will be captured by this fake access point.

On the other hand, through monitoring the traffic between the access point and particular WLAN clients, hacker may set up a fake WLAN client and mimics a valid WLAN client to access the network.

Built-in security features in WLAN

The following are some built-in security features for WLAN equipment:

SSID (Service Set ID)

SSID is a unique network identifier with a maximum of 32 characters. Each wireless access point has to be assigned with an SSID. The WLAN clients need to know the SSID of the access point to be connected with. The SSID can also be used to differentiate one WLAN from another. The access points and clients connected to a specific WLAN must use the same SSID.

WEP (Wired Equivalent Privacy)

As its name say, WEP is designed to provide an equivalent level of privacy in the wireless environment as it is in the wired environment. WEP uses a shared and static key, known to both access points and clients, to encrypt data packets before transmission. Up to 4 sets of static keys can be defined in access points/clients. WEP uses either a 40-bit or a 128-bit encryption mechanism for encryption. For most WLAN access points, WEP is disabled by default.

Security Risks of WLAN equipment

The built-in WLAN security features may have the following security risks:

SSID

By default, the access point will broadcast the SSID periodically for the clients to discover it. Also, the SSID is sent over the air in clear text in WLAN transmission. A hacker may scan easily for SSID and discover the availability of the access points.

Also, a WLAN access point may come with default SSIDs which are commonly known. Some of the default SSIDs are the name of the access point manufacturers such as Intel("intel"), Compaq ("compaq") and Linksys("linksys"). Other common SSIDs such as "wireless" and "wlan" are used in some other products.

WEP

The encryption mechanism of WEP is proved to be vulnerable. Tools are widely available on the Internet to hack WEP encryption. Also, the static key architecture in WEP poses security weakness: the key authentication follows hardware instead of the users. If the wireless client (e.g. notebook computer or PDA) is stolen or lost, the key for the school is automatically compromised. On the other hand, static key is easy to be hacked.

Managing the keys is not easy, especially in large wireless network. There is no easy way to protect the keys or to update them on a regular basis.

ACL

Spoofing of MAC address is possible. That is, a hacker can use devices to pretend he is a client with valid MAC address.

Also, the number of MAC address entries that an access point can support is limited. Managing the ACL would be quite difficult for wireless network with a large number of access points and clients. Also, distribution of MAC address entries to the access points would be tedious manual task.

ACL (Access Control List)

ACL (Access Control List) is used in some WLAN access points to control client access. The ACL is usually based on the client's wireless Ethernet MAC address which is unique in each client. The ACL is a database to store the MAC address that can access the WLAN. If the client's MAC address is not listed in the ACL, his/her access will be denied.

Suggested WLAN security measures

Here are some suggestions for enhancing the security of a wireless network. A general security set-up is good for any kinds of wireless network. An advanced security set-up may be applicable for wireless network with higher security requirements. However, it would incur a higher cost.

General Security Setup

No wireless device in SAMS network

- ❑ Wireless access point should **NOT** be connected directly to the SAMS network. Access points can only be used in other networks in schools such as the teaching and learning (ITED) network or MMLC network, but **NEVER** used in the administrative network such as SAMS.

SSID (Service Set ID)

- ❑ Change the default SSID immediately after installation. Never use the default SSID.
- ❑ Turn off the SSID broadcasting if the WLAN is not in use.
- ❑ Change the SSID regularly.

WEP (Wired Equivalent Privacy)

- ❑ Enable the WEP
- ❑ Never use the default WEP keys
- ❑ If possible, change the WEP key frequently

ACL (Access Control List)

- ❑ Use MAC filtering if your WLAN access point supports this function.

Access Point operations

- ❑ Change the default password for system administration. The default passwords are usually insecure, e.g. "public" is a common password in many access points.
- ❑ If possible, turn the access point power OFF when not in use for a considerable long period of time.
- ❑ Update the firmware of access points periodically.
- ❑ Do NOT connect the wireless access points to hubs in a wired network. Connect to switch can prevent easy sniffing.

Use static IP address for WLAN clients

- ❑ Do NOT use DHCP (dynamic host configuration protocol) for assigning IP address to WLAN clients. Use static IP addresses for WLAN clients. With DHCP enabled, the hackers can get applicable IP addresses for entry.

Audit the WLAN access points and clients regularly

- ❑ Keep good inventory and network records (e.g. IP addresses) for both WLAN access points and clients. Scan and audit regularly the WLAN equipment to ensure there is no rogue wireless connection.

Physical security of WLAN equipment

- ❑ Protect access points and WLAN cards from lost or stolen. The notebook computers with WLAN cards should be secured as they can be used to access the WLAN.

Advanced Security Setup

Use Firewall to separate WLAN network

- ❑ In this setup, a firewall/gateway is placed between the wired and wireless network. The traffic to the wired network would be screened by the firewall. This can minimize the risk of rogue WLAN clients getting into the wired network. Such setup is essential when there is important/restricted information in the wired network.

Use VPN (Virtual Private network)

- ❑ For high security requirement, VPN can be used to provide more secure data communication. Under VPN, users communicate in an encrypted tunnel between their devices and the wired or wireless LAN. (N.B. Schools may need to acquire additional VPN devices/software for VPN implementation.)

Summary

At present, wireless networks using the 802.11b protocol are inherently insecure and vulnerable. However, poor network configuration is usually the main cause that affects wireless LAN security.

In fact, it is impossible to completely eliminate the security risk of being hacked in a wireless system. However, the risk can be reduced significantly by adopting appropriate security measures. Although 802.11 has its vulnerabilities, schools themselves can mitigate WLAN security risks by education, careful planning, implementation, and management. Schools should also review the security policies of their wireless LAN from time to time to find out and prevent any security vulnerability of their WLAN. More security specifications are being proposed to enhance the security in 802.11 standard, such as 802.1x and 802.11i, to solve the static key, weak encryption and authentication problems. It is expected that the security weaknesses in WEP can be solved in later WLAN products.