

# Wireless LAN Security Policy

Version 1.0

08 June 2011



# 1. Introduction

A wireless local area network is a local area network without physical network wiring connections. The devices and computer in WLAN communicate each other using radio frequency electromagnetic airwaves. A WLAN can be configured 2 modes, namely ad-hoc mode and infrastructure mode. An ad-hoc WLAN allows computers to share their content (Files, Folders) by connecting directly to one another. In infrastructure mode computers share their resources through Wireless Access Point, which also interconnects the Wireless LAN and wired network. Business and government users are increasingly deploying wireless for mobility.

While WLAN provides greater mobility and flexibility, it also poses some security risks that are not face on wired networks. Unlike wired networks malicious users don't need physical access to WLAN, as the medium shared radio frequency. Current WLAN security implementations ensure proper access control and confidentiality of wireless communication. Service Set Identifier (SSID) and Wired Equivalent Privacy (WEP) were using to protect the wireless networks, but they can be broken in a short period of time.

With WLAN and the interdependencies of LGN wired network infrastructure, it is essential to ensure that the WLAN will not compromise the integrity, confidentiality and availability of LGN resources.

# 2. Object

This documentation will provide security guidance to implement WLAN for LGN sites. Site need should follow the guidelines specify here in the implementation of WLAN.

# 3. Scope

- ① Physical Security
- ② Confidentiality and Integrity
- ③ Key management
- ④ User authentication
- ⑤ Access Control
- ⑥ Client Security
- ⑦ User Awareness
- ⑧ Administration of Access Points
- ⑨ Availability
- ⑩ Login and Audit Trails

## 4. Security Threats

The security risks in WLAN are greater than those are in wired networks. Some new vulnerabilities are introduced by the weaknesses in wireless protocols. Following are the security threats that are in wireless networks;

- ① **Eavesdropping:** Intercepting the information that is transmitted over the WLAN is call eavesdropping. This can be done very easily now a day from a distance up to kilometers outside of the building perimeter without any physical connectivity to network. Intercepted information can be read if transmitted clear text or can be easily deciphered if only WEP encryption is used.
- ② **Traffic Analysis:** The intruder gain intelligence by monitoring the traffic pattern and deciphering the encrypted information by capturing the traffic flow. This may result in disclosure of sensitive data.
- ③ **Data Tampering:** The information transmitted over the WLAN can be deleted, replayed or modified by the attacker via man-in-the-middle-attack. This may result in a loss of data integrity and availability.
- ④ **Masquerading:** The attacker gain unauthorized access to the information and the network resources within the WLAN or other interconnected network by impersonating the identity of an authorized WLAN user. The intruder can create further havoc by launching attacks or malicious codes that will disrupt operations.
- ⑤ **Denial of service (DoS):** The attacker can jam up the entire frequency channel that is used for wireless data transmission using a powerful signal generator, microwave or massive network broadcasting traffic from a rouge wireless device. With high gain antennas and WLAN attack tools, the attacker can cause denial of service without close proximity to the targeted WLAN. Furthermore, it is not possible to locate the attacker base on current detection solutions. This attack can cause a denial of service and unavailability of information and network resources.
- ⑥ **Wireless Clients Attacks:** The attacker can potentially gain access to the information shared or stored in the wireless client when it was connected to an unprotected ad hoc WLAN or an untrusted third party WLAN. Furthermore, the compromised wireless client can potentially serve as a bridge to the corporate internal network, thus allowing perpetrator to gain access or launch attacks against the corporate internal network and resources.

## 5. Security Guidelines

The following is a set of security guidelines for LGN that would offer ample security in a wireless implementation. LGN Sites should flow these guidance in order to implement successful secure wireless network. However this paper does not specifically address the security of wireless applications such as Wireless Applications Protocol (WAP) enabled systems, mobile wireless (e.g. PDA security) or Wireless WAN (e.g. GSM, CDMA security), though the security recommendations given here might generally be applicable in some areas.

### 5.1 Physical security

- ① The wireless station and its WLAN adaptor card should not be physically exposed to prevent theft and unauthorized access to the WLAN.
- ② The access points should be placed within the physically protected office environment to prevent them from any unauthorized access and physical tampering. Security alarm system can also be used wherever applicable.
- ③ The access points should be physically located away from external sources of electromagnetic interference, e.g. microwave ovens.
- ④ The access point should be kept in a weatherproof container if they are located in the open area. Any physical harm on the access point can possibly disrupt the network services and information resource via the WLAN.
- ⑤ A site review should be conducted to assess the coverage of WLAN to minimize spillage of WLAN traffic beyond the physical office environment. The review would help to determine the physical security of the WLAN environment, e.g. the ease of spoofing by the public.

### 5.2 Confidentiality and Integrity

- ① Confidential or important information should not be transmitted unprotected over the WLAN.
- ② The information should be encrypted prior to transmission over the WLAN.
- ③ WEP encryption should not be used as the only form of protection to ensure the confidentiality and integrity of the information transmitted over the WLAN.
- ④ Network or end-to-end encryption such as VPN should be used to protect important information during transmission. Cryptographic hashing function such as MD5 or SHA-1 can also be used to ensure integrity of the information transmitted over the WLAN.

## 5.3 Key Management

- ① The symmetric encryption keys, e.g. the WEP keys stored in the access points and wireless stations, should be protected from unauthorized access.
- ② Strong symmetric encryption, e.g. using 128-bit key length, should be used to protect the information that is transmitted over the WLAN.
- ③ The encryption keys should be changed periodically, e.g. once every 90 days.
- ④ When available, dynamic keys should be used to mitigate the security risks that are inherent with the use of shared static keys, e.g. exposure or theft of static encryption keys stored in the access points and wireless stations, dictionary attack on the sniffed data traffic.
- ⑤ The symmetric encryption keys should be protected during key distribution to the users.
- ⑥ The new keys should be sent to the users either in encrypted form or through other secure means to prevent unauthorized access to the keys during transit.
- ⑦ The symmetric encryption keys should be loaded directly into the access point without traversing any intermediary networks. If direct key loading is not possible, the symmetric encryption keys should be securely loaded into the access point via the wired network without going through the WLAN.

## 5.4 User Authentication

The access control mechanisms supported by the WLAN technology, e.g. using the ESSID, the MAC address and the WEP key, only verify authorized wireless stations but not the users. As such, unauthorized personnel can gain access to the WLAN and its network resources using a stolen wireless station. Where the identity of the user needs to be verified, user authentication mechanisms such as users' ids/passwords, smart cards, security tokens, should be used to prevent unauthorized access to the LGN internal network via the WLAN.

## 5.5 Access Control

- ① The access point should be configured to allow only authorized wireless stations to associate with the WLAN.
- ② Only authorized wireless stations, which have the same network name or Extended Service Set ID (ESSID), authorized Media Access Control (MAC) address and WEP Shared Key, should be allowed to access the WLAN.
- ③ The access point should be configured to drop any unencrypted network traffic.
- ④ Existing network or application level access control and user authentication should be maintained to prevent unauthorized access to the internal wired network and applications in the event that the security of the WLAN has been compromised.
- ⑤ Access control mechanisms such as firewalls should be implemented to segregate the WLAN from the internal wired network.
- ⑥ The WLAN should be deployed in a different network segment, which is separate from the internal wired network.
- ⑦ Network or IP filtering can be implemented at the gateway to ensure that only authorized network traffic from the WLAN or legitimate access points are allowed to enter the wired network.

## 5.6 Client security

- ① Access control and intrusion detection mechanisms should be installed on the wireless station where possible.
- ② The user's privileges and access rights to the systems and network resources should be restricted if they access via the WLAN using client computing devices where there are no controls available, e.g. PDAs. Software programs that can be used to configure the wireless station as an access point should be removed to minimize set-up of rogue access points.
- ③ The wireless station should not be configured for network file sharing without any protection to prevent any unauthorized access to his local files.

## 5.7 User Awareness

- ① The LGN users should not be allowed to set up their wireless stations in ad-hoc mode and communicate with each other without going through the access point.
- ② The user should power down the wireless station when it is not being used for a long period of time, e.g. after office hours.
- ③ The user's wireless station should not have concurrent direct connection to any untrusted network, e.g. the Internet, when the wireless station is connected to the internal wired network.

## 5.8 Administration of access points

- ① The access to WLAN key distribution program should be controlled and limited to the administrators only.
- ② The built-in COM ports of the access point should be disabled or password-protected.
- ③ All unnecessary services and ports in the access points should be removed or closed.
- ④ The default Service Set ID (SSID) of each access point should be changed.
- ⑤ If possible, SSID should not be broadcasted.
- ⑥ The default SNMP community string should be changed if the access point has SNMP agent running on it.
- ⑦ The access point should not be directly connected to a network device that can potentially broadcast all data packets to all connected network devices on the wired and wireless networks.
- ⑧ Periodic scanning on the WLAN should be conducted to detect the presence of rogue access points, unauthorized ports/services or any security vulnerabilities in the network.
- ⑨ The password for remote management of access points can be captured and used to gain unauthorized access to the access points. As such, administration of access points should not be done over the WLAN. Instead, the access points should be administered via the wired network or locally via the access point's built-in COM ports.
- ⑩ The user should be required to report the loss of his wireless station and WLAN adaptor card immediately to site administrator or relevant person.
- ⑪ The WLAN adaptor card should be returned to the LGN upon staff resignation or termination to prevent the user from gaining unauthorized access to the WLAN.
- ⑫ The users should not be allowed to install or run any unauthorized network software on their PCs.

## 5.9 Availability

The WLAN is vulnerable to denial of service attacks such as network jamming. As such, it should not be used as the only means to access the LGN network and systems. Load balancing across multiple access points should be implemented to mitigate the risk of an access point being inaccessible due to flooding of network packets at a particular access point.

## 5.10 Logging and Audit Trails

- ① Unauthorized network traffic and access to the WLAN should be logged, e.g. using Intrusion Detection System, to detect attacks directed over the WLAN.
- ② Any exceptions or abnormal network activities should be logged and alerts sent to the administrators, as per the LGN security incident response plan. Information such as source/destination IP addresses, MAC addresses, user's logon names/ids and logon time/duration, can be logged to aid analysis and investigation.

## 6. Summary

Following will provide the summary of wireless LAN implementation guidelines,

- Wireless access points, adaptor cards should be physically secured.
- Encryption should be used when transmitting information through WLAN.
- Should not rely on a single encryption mechanism e.g. WEP encryption.
- Should use strong encryption key length to protect the information that is transmitting over the WLAN.
- Should change the encryption keys periodically and if possible dynamic encryption keys should be used.
- New encryption keys should be protected during the distribution.
- User authentication mechanisms like (username/password, secure tokens) should be used when user connect to the WLAN.
- The access point should be configured to allow only authorized wireless stations to associate with the WLAN.
- Access control mechanisms such as firewalls should be deployed.
- Intrusion detection mechanisms and user privilege levels should be implemented on client side of the WLAN.
- Should not allow users to use ad-hoc mode on their wireless stations and should power down the wireless station when it is not using for long period of time.
- Controlling the access point should be done only by an administrator and all ports that are not using on the access point should be disabled or password protected.
- Periodic scanning on the WLAN should be conducted.
- Administration of access points should not be done over the WLAN.
- Logs should be enabled on access point to detect unauthorized network traffic and access.