CyberSecurity MALAYSIA

An agency under MOSTI

Wireless Local Area Network (LAN) Security Guideline

Noor Aida Idris
Mohamad Nizam Kassim

Securing Our Cyberspace

“To say a system is secure because no one is attacking it is very dangerous”

(Microsoft Founder, Bill Gates)

COPYRIGHT

REGISTERED OFFICE:

CyberSecurity Malaysia,
Level 7, Block A, Mines Waterfront Business Park,
No 3, Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor, Malaysia
Phone: +603 - 8992 6888
Fax: +603 - 8945 3205
http://www.cybersecurity.my

Printed in Malaysia

ACKNOWLEDGEMENT

CyberSecurity Malaysia wishes to thank the Panel of Reviewers who reviewed the drafts of this guideline and contributed to its content.

External Reviewers

1. A Fattah Yatim (Teknimuda (M) Sdn Bhd)
2. Abdul Aziz Hassan (Malayan Banking Berhad)
3. Abdul Rahman Mohamed (Malaysia Airlines)
4. Adnan Mohamad (Bank Negara Malaysia)
5. Azleyna Ariffin (Jaring Communications Sdn Bhd)
6. David Ng (Jaring Communications Sdn Bhd)
7. Dr Jamalul-lail Ab Manan (MIMOS Berhad)
8. Louie Low (Genting Group)
9. Mahdi Mohd Ariffin (Bank Negara Malaysia)
10. Mahizzan Mohd Fadzil (Maxis)
11. Ong Ai Lin (PricewaterhouseCoopers)
12. Prof Dr Shahrin Sahib@Sahibuddin (Universiti Teknikal Malaysia Melaka)
13. Thaib Mustafa (Telekom Malaysia Berhad)
14. Ummi Kalsom Abdul Rahim (Securities Commission)
15. Yusfarizal Yusoff (Time dotCom Berhad)

Internal Reviewers

1. Abdul Fuad Abdul Rahman (Security Assurance)
2. Adli Abd Wahid (Malaysian Computer Emergency Response Team)
3. Aswami Fadillah Mohd Ariffin (Digital Forensic)
4. Ida Rajemee Ramli (Security Management & Best Practices)
5. Maslina Daud (Security Management & Best Practices)
6. Nor Aza Ramli (Security Management & Best Practices)
7. Muralidharon (Security Management & Best Practices)
8. Nor'Azuwa Muhammad Pahri (Security Assurance)
9. Raja Azrina Raja Othman (Chief Technology Officer)
10. Ruhama Mohd Zain (Security Assurance)
11. Suhairi Mohd Jawi@Said (Malaysian Computer Emergency Response Team)
12. Wan Roshaimi Wan Abdullah (Security Assurance)
13. Zahri Yunos (Chief Operating Officer)

Table of Contents

EXECUTIVE SUMMARY

The emergence of the wireless networking standard (e.g. IEEE 802.11) has contributed to the popularity of wireless local area network (LAN) deployment in many organisations. While wireless LAN provides greater mobility and flexibility, it also poses security risks to the organisations. The *'Wireless Local Area Network (LAN) Security Guideline'* focuses on information security issues in wireless LAN, and recommends a set of security controls to help organisations secure their wireless LANs. There are 3 aspects of security controls described in this Guideline: Management, Technical and Operational controls.

Management controls for securing wireless LAN involve senior management's support i.e. defining roles and responsibilities, producing a comprehensive set of security policies and procedures, and conducting risk assessments and wireless network assessments. Technical controls, meanwhile, involve the use of hardware and software solutions in securing the wireless LAN environment. Wireless client protection, access points protection, wireless encryption, radio frequency interface monitoring, wireless equipment inventory, and wireless connectivity management are included in technical controls. Operational controls include physical and environmental protection, human resource security, training and awareness programs, patch management, and an incident handling and response management.

Organisations are recommended to combine management controls with operational and technical controls. These three security controls, when adequately implemented and configured, can be effective in reducing information security risks in organisational wireless LANs.

1

INTRODUCTION

Wireless local area network (LAN) technology are widely deployed and used in organisations today. A wireless LAN is a flexible data communications system implemented as an extension to, or as an alternative for, a wired network. Using radio frequency (RF) technology, wireless LANs transmit and receive data over the air, minimising the need for wired connections. Thus, wireless LANs combine data connectivity with user mobility.

Today wireless LANs are becoming more widely recognized as a general-purpose connectivity alternative for many organisations and home users. Wireless LAN users can access shared information without looking for a place to plug in, and network administrators can set up networks without installing physical cables. However, organisations should be aware of threats in wireless LANs, and learn how to manage information security risks in wireless LANs effectively.

1.1 OBJECTIVE

The objective of *'Wireless Local Area Network (LAN) Security Guideline'* is to guide organisations in securing their wireless LANs. The Guideline provides recommendations on three security controls that organisations should implement. The recommendations are in line with relevant standards and/or findings from vulnerability assessments by CyberSecurity Malaysia.

This Guideline provides advice and guidance only; as such no penalties are imposed for organisations that do not follow them. It is also not intended to replace any existing information on security standards and/or guidelines produced by standards organisations or regulators.

1.2 SCOPE

The scope of this Guideline is three security controls: Management, Technical, and Operational control, which organisations should implement in securing their wireless LAN. The three security controls discussed in this Guideline are directly related to information security aspects in wireless LAN only.

The wireless LAN referred to in this guideline is the IEEE 802.11 which denotes a set of wireless LAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802) [1].

However, certain organisations may have additional or specific requirements (which are derived from international, local, organisational, and/or government regulations) that are applicable to them. These additional requirements are not within the scope of this guideline.

1.3 TARGET AUDIENCE

This Guideline is recommended for the following:

- Organisations that plan, develop, implement or assess their wireless LAN.
- Individuals who are system and network administrators, who design, deploy, administer and maintain organisational wireless LANs.
- Individuals who are information security or network security personnel with information system and monitoring responsibilities on organisational wireless LANs.

[1] http://www.wirelesslans.org

- Individuals who are internal and external auditors, information security officers or security consultants who perform security assessments on organisational wireless LANs.

1.4 DOCUMENT STRUCTURE

This Guideline is structured as follows:

- Section 1 introduces objective, scope and target audience of the Guideline.
- Section 2 defines Terms and Definitions used in the Guideline.
- Section 3 lists Acronyms and Abbreviations in the Guideline.
- Section 4 provides an overview of the wireless LAN, including its operating mode, benefits, and threats to organizations.
- Section 5, 6 and 7 describe three security controls required in wireless LAN which are Management, Technical, and Operational controls.
- Appendix A provides a checklist of security controls described earlier in the Guideline.
- Appendix B provides a table of summary for IEEE 802.11 standards.

2

TERMS & DEFINITIONS

For the purpose of this Guideline, the following terms and definitions apply.

2.1
ACCESS POINT

A device that logically connects wireless clients operating in an infrastructure to one another, and provides access to the distribution system, if connected, which is typically an organisation's enterprise wired network [2].

2.2
AD-HOC NETWORK

A wireless network that dynamically connects wireless clients to each other without the use of an infrastructure mode's device, such as an access point [3].

2.3
ATTACKER

Someone who breaks into someone else's computer system, often a network, bypasses passwords or licenses in computer programs, or in other ways intentionally breaches computer security. Attackers can do this for profit, maliciously, for an altruistic purpose or cause, or because the challenge is there [4]. Also known as cracker.

2.4
COMPUTING RELATED EQUIPMENT

Computer, network, telecommunications and peripheral equipment that support the information processing activities of an organisation. Examples of computing related equipments are computers, personal digital assistants (PDAs), thumb drives, printers, video cameras, game consoles and multimedia devices.

2.5
FIREWALL

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. The term also implies the security policy that is used with the programs [5].

2.6
INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT) SYSTEM

A set up consisting of hardware, software and firmware of computing related equipment, and the people who use them. An ICT system includes any computing related equipment or other electronic information handling systems and associated equipment, or interconnected systems that are used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data/information.

---

2 NIST SP 800-48r1 Guide to Securing Legacy IEEE 802.11 Wireless Networks
3 NIST SP 800-48r1 Guide to Securing Legacy IEEE 802.11 Wireless Networks
4 http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211852,00.html
5 http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212125,00.html

2.7
INFORMATION SECURITY

Preservation of confidentiality, integrity and availability of information; other properties such as authenticity, accountability, non-repudiation and reliability may be included [6].

2.8
INFRASTRUCTURE NETWORK

A wireless network that requires the use of an infrastructure device such as an access point, to facilitate communication between wireless clients [7].

2.9
MALICIOUS CODE

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system, or intentionally annoying or disrupting the victim [8].

2.10
MEDIA ACCESS CONTROL

A unique 48-bit value that is assigned to a particular wireless network interface by the manufacturer [9].

2.11
ORGANISATIONS

Public or private registered entities.

2.12
PATCH

A piece of software designed to update or fix problems with a computer program or its supporting data. This includes fixing bugs, replacing graphics, and improving the usability or performance.

2.13
RANGE

The maximum possible distance for communicating with a wireless network infrastructure or wireless client [10].

2.14
RISK ASSESSMENT

An initial and periodical step in the risk management process, risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognised threat [11].

2.15
ROGUE ACCESS POINT

An unauthorized Access Point that do not meet the documented or implied organizational requirements for wireless networks [12].

2.16
SERVICE SET IDENTIFIER (SSID)

A name assigned to a wireless local area network that allows wireless clients to distinguish one wireless local area network from another [13].

---

6 ISO/IEC 27001:2005 Information Security Management Systems
7 NIST SP 800-48r1 Guide to Securing Legacy IEEE 802.11 Wireless Networks
8 NIST SP 800-83 Guide to Malware Incident Prevention and Handling
9 ISO/IEC 27001:2005 Information Security Management Systems
10 ISO/IEC 27001:2005 Information Security Management Systems
11 ISO/IEC 27001:2005 Information Security Management Systems
12 http://www.rogueap.com/rogue-ap-docs/RogueAP-FAQ.pdf
13 ISO/IEC 27001:2005 Information Security Management Systems

2.17
THREAT
A probable impending danger or warning of impending danger where vulnerability may be exploited to cause harm to wireless LANs.

2.18
VIRTUAL PRIVATE NETWORK
A means by which certain authorised individuals (such as remote employees) can gain secure access to an organisation's intranet by an extranet (a part of the internal network that is accessible via the Internet) [14].

2.19
VULNERABILITY
A weakness in an ICT system that allows an attacker to violate the integrity of the ICT system in a wireless network.

2.20
WIRELESS CLIENT
A computing related equipment in a wireless local area network.

2.21
WIRELESS LOCAL AREA NETWORK (LAN)
A group of wireless access points and associated infrastructure within a limited geographic area, such as an office building or building campus, that is capable of radio communications. Wireless LANs are usually implemented as extensions of existing wired LANs to provide enhanced user mobility [15].

2.22
WIRED EQUIVALENT PRIVACY
A security protocol, specified in the IEEE 802.11 standard, that is designed to provide a wireless local area network with a level of security and privacy comparable to what is usually expected of a wired local area network. WEP is no longer considered a viable encryption mechanism due to known weaknesses [16].

2.23
IEEE 802.11i
An IEEE standard specifying security mechanisms for 802.11 networks. 802.11i makes use of the Advanced Encryption Standard (AES) block cipher. The standard also includes improvements in key management, user authentication through 802.1X and data integrity of headers. (802.1X, AES, WPA2)

Wi-Fi Alliance is a governing body that introduce WPA/WPA2 security standards.

2.24
WPA/WPA2
Wi-Fi Protected Access, a specification adopted from the 802.11i specification by the Wi-Fi Alliance to promote an improved interoperable security mechanism for wireless network [17].

---

14 NIST SP 800-48 Wireless Network Security 802.11, Bluetooth and Handheld Devices
15 NIST SP 800-48r1 Guide to Securing Legacy IEEE 802.11 Wireless Networks
16 NIST SP 800-48r1 Guide to Securing Legacy IEEE 802.11 Wireless Networks
17 http://www.wi-fi.org/knowledge_center_overview.php?type=3

3

ACRONYMS AND ABBREVIATIONS

Selected acronyms and abbreviations used in the Guideline are defined below.

ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
CISO	Chief Information Security Officer
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
DES	Data Encryption Standard
DoS	Denial of Service
EAP	Extensible Authentication Protocol
GPS	Global Positioning System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPSec	Internet Protocol Security
ISO	International Organisation for Standardisation
IT	Information Technology
LAN	Local Area Network
MAC	Medium Access Control
NIC	Network Interface Card
PC	Personal Computer
PCI	Peripheral Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
RADIUS	Remote Authentication Dial-in User Service
RF	Radio Frequency
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket Layer
TLS	Transport Layer Security
TKIP	Temporal Key Integrity Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WNIC	Wireless Network Interface Card
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

4

OVERVIEW OF WIRELESS LOCAL AREA NETWORK

Wireless local area networks (LAN) are groups of wireless networking nodes within a limited geographic area, such as an office building or building campus, that are capable of radio communication [18]. Wireless LANs are usually implemented as extensions to existing wired local area networks to provide enhanced user mobility and network access. This enables organisations to offer its employees the mobility to move around within a broad coverage area and still be connected to the network.

The most widely implemented wireless LAN technologies are based on the IEEE 802.11 standard and its amendments. The original 802.11 standard was published in June 1997 as IEEE Std. 802.11-1997, and it is often referred to as 802.11 Prime because it was the first WLAN standard. The standard was revised in 1999, reaffirmed in 2003, and published as IEEE Std. 802.11-1999 (R2003). Please refer to Appendix A for the summaries of various IEEE802.11 standards.

Wireless LAN offers a quick and effective extension of a wired network or standard LAN. Installing a wireless LAN is easy and eliminates the need to pull wired cables through walls and ceilings.

4.1 WIRELESS LAN COMPONENTS

The two fundamental components in wireless LAN are access points and wireless clients.

4.1.1 Access points

Access points (APs) are base stations for the wireless network. They transmit and receive radio frequencies for wireless clients to communicate with.

4.1.2 Wireless Clients

Wireless clients can be any computing related equipment device such as laptops, personal digital assistants, and IP phones, or fixed devices such as desktops and workstations that are equipped with a Wireless Network Interface Card (WNIC).

4.2 WIRELESS LAN OPERATING MODE

A wireless LAN can be configured in either ad-hoc mode (Figure 1) or infrastructure mode (Figure 2).

4.2.1 Ad-Hoc Mode

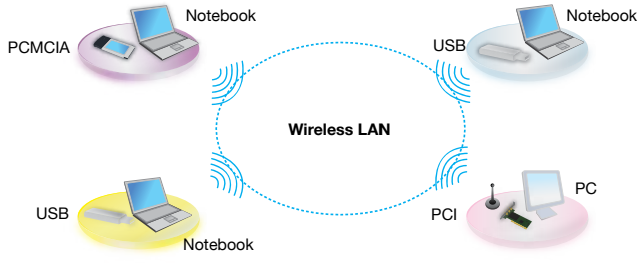

Figure 1 – Ad-hoc Mode

[18] NIST SP800-48r1 Guide to Securing Legacy IEEE 802.11 Wireless Networks

An ad-hoc wireless LAN mode allows wireless clients to connect directly to one another to share files or resources. This mode does not require a wireless access point; hence the wireless clients connect and communicate directly to each other (within a certain range) via a wireless client device (e.g. wireless USB, PCI, PCMCIA, PC card adapters, and built-in wireless chips). This mode is established by several wireless clients, which have the same SSID and radio channel for a peer-to-peer communication mode.

4.2.2 Infrastructure Mode

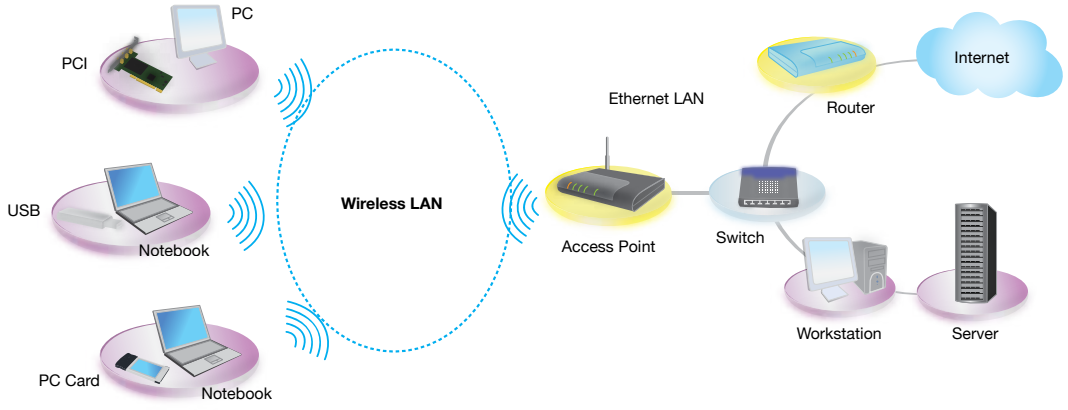

Figure 2 – Infrastructure Mode

Infrastructure mode must contain at least one wireless access point that connects wireless clients to wireless LANs or other networks such as the Internet or intranet. The wireless access point establishes an infrastructure mode for networking between all wireless clients and wired network resources (i.e. servers, printers).

4.3 BENEFITS OF WIRELESS LAN TO ORGANISATIONS

Wireless LAN offers organisations the following benefits:

1. **Mobility** – Organisations provide employees with convenience to access online resources and the Internet without a network cable.
2. **Rapid deployment** – Organisations reduce time involved in implementing wireless LANs due to reduction in need to lay out or pull physical cables through walls and ceilings.
3. **Flexibility** – Organisations enjoy flexibility of setting up and removing wireless LANs in many locations, i.e. temporary locations for conferences and seminars.
4. **Scalability** – Organisations easily increase the network coverage from small ad-hoc networks to very large infrastructure networks by putting an access point.

4.4 WIRELESS LAN THREATS

As many organisations have implemented wireless networks and as the numbers continues to grow, it becomes crucial for them to learn and understand the types of threats in wireless LANs. Organisations, therefore, need to understand security threats before implementing wireless LANs by carrying out further studies in understanding threats associated with wireless LANs.

The threats described here are relevant to wireless LANs in general [19]:

1. **Denial of Service** – Attacker prevents or limits the normal use or management of wireless networks or network devices.
2. **Eavesdropping** – Attacker passively monitors wireless networks for data, including authentication credentials.
3. **Man-in-the-Middle** – Attacker actively intercepts communications between wireless clients and APs, thereby obtaining authentication credentials and data.
4. **Masquerading** – Attacker impersonates an authorised user and gains certain unauthorised privileges to wireless networks.
5. **Message Modification** – Attacker alters a legitimate message sent via wireless networks by deleting, adding to, changing, or reordering it.
6. **Message Replay** – Attacker passively monitors transmissions via wireless networks and retransmits messages, acting as if the attacker was a legitimate user.
7. **Traffic Analysis** – Attacker passively monitors transmissions via wireless networks to identify communication patterns and participants.
8. **Physically Tampered** – Passwords can be retrieved from the hardware due to changes to the AP's antenna or when the AP is moved to another location. This increases the signal strength in favour of the attacker).

With the identified threats in a wireless network, and others that may prevail, there is a need for organisations to apply the following recommended security controls in protecting computers and securing wireless LANs in their organisations. Without implementing appropriate security controls, many opportunities will abound for attackers to impose threats to an organisation's wireless network.

4.5 SECURITY CONTROLS IN WIRELESS LANs

Security controls is a suite of security safeguards or countermeasures to be established by organisations to protect the confidentiality, integrity and availability of their information system and information[20].

Security controls provide a means of managing risks that include, but are not limited to, policies, procedures, guidelines, practices or organisational structures, which can be of administrative, technical, management, or legal nature [21]. Therefore, security controls for wireless LANs can be selected from a variety of areas (including risk management, personnel security, media protection, physical and environmental protection, contingency planning, incident response management, etc.) to ensure a holistic approach to securing wireless LANs in organisations.

For this Guideline, security controls are grouped into three categories: Management, Technical, and Operational controls.

Management controls are security controls that focus on management of risk and information system security [22]. The management needs to understand the objectives, benefits, threats and vulnerabilities, as well as risks, before deciding on the deployment of a wireless LAN in an organisation. Once the decision is made, the management shall identify strategies and security controls to prevent any compromise to the wireless LAN. However, the management controls cannot work independently; it should and usually is complemented by two other aspects: technical and operational.

Technical controls are security controls which are primarily implemented and executed through mechanisms contained in computing related equipments (hardware, software, or firmware components of the system) [23]. They involve the use of countermeasures or safeguards which are already incorporated into computing related equipments or wireless devices.

---

19 NIST SP800-48r1 Guide to Securing Legacy IEEE 802.11 Wireless Networks
20 NIST FIPS 199, "Security Controls"
21 ISO/IEC 27002:2005 Code of Practice for Information Security Management
22 NIST FIPS Publication 200 Minimum Security Requirements for Federal Information and Information Systems
23 NIST FIPS Publication 200 Minimum Security Requirements for Federal Information and Information Systems

Operational controls are security controls which are primarily implemented and executed by people (as opposed to systems) [24]. They involve providing security awareness and training to employees, and securing the physical premise which houses the wireless LAN facilities and/or devices. These controls need to be implemented by organisations continuously throughout the year to ensure wireless network risks can be identified and mitigated effectively to reduce their impact to organisations.

These three security controls, Management, Technical, and Operational are to be used together not just to mitigate security risks in wireless LANs, but also to ensure the preservation of confidentiality, availability and integrity of transactions, and data transmitted via wireless LANs. A full explanation of these security controls are elaborated in the following sections.

24 NIST FIPS Publication 200 Minimum Security Requirements for Federal Information and Information Systems

5

MANAGEMENT CONTROLS

Management controls are very much required to ensure that a secure wireless LAN is implemented in organisations. To ensure this, roles and responsibilities for wireless LAN planning and implementation are to be clearly defined. Security policies and procedures related to wireless LANs need to be developed and endorsed. Senior management has to ensure that risk assessment on wireless LANs and wireless network assessments are conducted periodically and in accordance to organisational policies and procedures, as well as other security requirements.

5.1 ROLES AND RESPONSIBILITIES

Security is not a task; it is a continuous process that every employee in organisations should understand and undertake in their job functions. To ensure adequate security in wireless LANs, senior management should play significant roles in network security especially related to wireless networks.

The following tasks should be used as guidance in identifying the roles and responsibilities in ensuring wireless LAN security:

1. Senior management should provide support for planning and implementing security for wireless LANs through clear direction and demonstrated commitment.
2. Senior management should ensure risk assessment is performed before implementing wireless LANs (Refer to Section 5.3 *Risk Assessment of Wireless LAN* for further information).
3. The Human Resources (HR) department (together with senior management) should engage a dedicated employee (e.g. CISO) who is independent of the Information Technology (IT) department to oversee the organisation's information security, especially wireless network security.
4. The HR and IT departments (together with senior management) should define roles and responsibilities of each employee allowed to use wireless devices, network, and facilities, in an employee's terms and conditions.
5. All employees should be aware of technical and security implications of wireless and handheld device technologies by attending training and awareness sessions held by organisations.

5.2 POLICIES AND PROCEDURES

Security policies and procedures related to wireless LANs should be developed, documented, approved and maintained based on security requirements, best practices and agreed fundamental guidelines set forth by organisations.

A policy is typically a document that outlines overall intention and direction as formally expressed by management [25]. Comprehensive wireless security policies and procedures for organisations, and compliance therewith, is the minimum requirement needed in organisations to plan and implement wireless LANs. Its main purpose is to inform employees on what is deemed as allowable and what is not with regards to wireless LANs.

The IT department should develop policies and procedures related to wireless LAN security; and ensure they are approved and endorsed by senior management. The endorsed policies and procedures should be communicated accordingly to all employees. In addition, these policies and procedures should be reviewed periodically to ensure its effectiveness and suitability.

25 ISO/IEC 27002:2005 Code of Practice for Information Security Management

The following statements should be included in a wireless LAN's security policy [26] (Note: this is not an exhaustive list):

1. Identify who may use wireless LAN technology in the organisation (please refer to Section 5.1 (4)).
2. Identify whether Internet access is required.
3. Describe who is responsible to install wireless access points and other wireless equipments for the organisation.
4. Provide limitations on the location of physical security for wireless access points.
5. Describe the type of information that may be sent over a wireless network.
6. Describe conditions under which wireless devices are allowed.
7. Define standard security settings for wireless access points.
8. Describe hardware and software configurations for all wireless devices.
9. Provide guidelines for the protection of wireless clients to minimise/reduce theft. (This is because an employee is responsible to protect their wireless clients.)
10. Provide guidelines on the use of encryption and key management for wireless clients.

5.3 RISK ASSESSMENT OF WIRELESS LANs

A risk assessment is the process of identifying, quantifying and prioritising risks against criteria for risk acceptance and objectives relevant to the organisation [27].The primary goal of a risk assessment for wireless LANs is to mitigate impacts of possible threats in a wireless network. A risk assessment of wireless LANs should be performed periodically or when there are any changes that impact an organisation's wireless LAN.

Organisations should define the approach, scope and methodology on conducting risk assessments for wireless LANs and perform risk assessments on wireless LANs periodically to fully explore the security posture of their wireless network. A risk assessment report should then be produced which identify risks and security controls to be implemented in mitigating them.

Organisations should consider the wireless LAN's threats, vulnerabilities and impact of confidentiality, integrity and availability of information, when doing a risk assessment of wireless LANs. The following areas should be included in the risk assessment's scope for wireless LANs (Note: This is not an exhaustive list, other areas can be included).

1. Policies and procedures

Does the existing organisation's policies and procedure allow employees to access the organisation's network remotely from public wireless hot spots? Does it describe adequate protection on the wireless network, i.e. encryption and authentication mechanisms?

Policies and procedures provide a benchmark for determining whether or not organisations comply with their own set of rules. Reviewing current policies and procedure related to wireless LANs will ensure they do not provide ways for an attacker (e.g., a disgruntled employee) to access wireless networks unknowingly or harm company resources.

2. Location of Access Points

Where are access points placed? Will the wireless signal extend beyond physical boundary of organisations and their controls?

Organisations should locate wireless access points in their wireless network. This can be done by interviewing IT personnel and random staff, and reading through related documentation to gain an understanding of the wireless system's architecture and configurations of access points. In addition, an organisation should search and scan for rogue (unauthorised) access points as part of the assessment.

[26] NIST SP 800-48 Wireless Network Security, 802.11, Bluetooth and Handheld Devices
[27] ISO/IEC 27001:2005 Information Security Management Systems

3. **Types of wireless transactions**
   What types of data will the wireless LAN transmit? What are security measures to be applied if the transaction contains private and confidential data?

   Organisations should decide which data is allowed to be transmitted over wireless networks. A wireless LAN that transmits e-mails, corporate data and database traffic requires more complex security methods (e.g. SSL encryption) than one that transmits encrypted data.

4. **Wireless LAN users**
   Who should have access to the organisation's wireless LAN? Is it all employees or senior management only? What are security measures to be applied if the users include vendors?

   Employees who are authorised to access an organisation's wireless LAN should be aware of security policies and procedures, especially on installation of wireless LAN components. A new employee, for example, may install wireless access points on the organisation's network (without any security settings enabled).

5. **Dependency on wireless LAN infrastructure**
   How critical is a wireless LAN in the organisation? Does the organisation have backup connections in case of wireless LAN failure or intrusion?

   Organisations should prepare and produce a contingency plan should a critically used wireless LAN cause congestion. At the same time, the plan should cover security and not compromise the organisation's confidential information.

5.4 WIRELESS NETWORK ASSESSMENT

A wireless network assessment highlights vulnerabilities found in current wireless LAN implementations in organisations. The wireless network assessment can be performed either randomly or on fixed schedules. To maintain the independence of the assessment results, wireless network assessments shall be performed by an independent and trusted third party. This assessment can and should be part of the periodic risk assessment effort to ensure potential wireless LAN threats and vulnerabilities are mitigated.

The following tasks should be used as guidance for conducting a wireless network assessment:

1. Produce security requirements for conducting a wireless network assessment.
2. Define objective, scope and frequency of the assessment based on the security requirements.
3. Produce roles and responsibilities of the employees, contractors, and/or 3rd party users (if applicable) who are involved in the assessment.
4. Carry out the wireless network assessment after obtaining approval from senior management.

5.4.1 War-Driving

Organisations can perform war-driving as one of the methods to assess its wireless network. War-driving is an activity to detect the existence of wireless LANs by locating wireless access points [28].

The basic war-driving kit consists of the following:

- Computer (or notebook)
- Wireless NIC
- Software
- Antenna (optional)
- Global Positioning System (GPS) unit (optional)

[28] http://www.wardrive.net/

6

TECHNICAL CONTROLS

Technical controls are security controls that are very much related to technical tools and software that can be used by organisations. These controls should be implemented along with management and operational controls. The technical controls in securing wireless LANs include, but are not limited to, wireless client protection, AP protection and types of wireless encryption.

6.1 WIRELESS CLIENT PROTECTION

Appropriate protection needs to be applied to wireless clients in order to secure wireless communications. To secure these wireless clients, organisations should ensure that encryption, malicious code protection software, personal firewall software, windows preferred network list (PNL), and wireless radio interface are installed and enabled at employees wireless clients.

6.1.1 Encryption

Wireless clients should be configured with strong encryption. This is to ensure that confidential data being transmitted from wireless clients are secure.

The following tasks should be used as guidance when configuring wireless clients with strong encryption:

1. Install and use encryption software such as VPN, IPSec and SSL to encrypt wireless data traffic at application layer. (Regardless of types of security mechanism implemented at APs, it is recommended that all wireless clients consider application layer encryption in protecting data that is transmitted over the wireless network.)

6.1.2 Malicious Code Protection

Wireless clients should have protection against malicious codes. Malicious code protection software is a program (i.e. anti-virus software, anti-spyware software, etc.) that provides protection against several forms of malicious codes including viruses, logic bombs, Trojan horses, worms, and back door attacks i.e. by passing normal authentication and securing remote access to a network.

The following tasks should be used as guidance in installing malicious code protection to protect a wireless client:

1. Ensure wireless clients accessing the wireless LAN are installed with malicious code protection software.
2. Configure the software (upon installation) to automatically download and apply updated patches accordingly.
3. Schedule a full scan of malicious codes periodically at the wireless client during periods of low activity.

6.1.3 Personal Firewall Protection

Wireless clients should have personal firewall software installed. Personal firewall software prevents malicious traffic from penetrating wireless clients, which can subsequently reach other wireless clients or hosts on the wireless network.

The following tasks should be used as guidance in installing a personal firewall to protect wireless clients:

1. Ensure that wireless clients accessing the wireless LAN have personal firewalls installed.
2. Configure (upon installation) the software to automatically download and apply updated patches accordingly.

6.1.4 Windows Preferred Network List (PNL)

Wireless clients should manage wireless networks that they wish to automatically connect to, via Windows PNL. Windows PNL contains a list of wireless networks that the wireless client "knows" about (or has ever known about). If multiple networks can be available simultaneously, this list can be rearranged in any preferred order. The networks which appear at the top of the list are the most preferred network, with the least preferred at the bottom.

The following tasks should be used as guidance in managing Windows PNL to protect wireless clients:

1. Ensure that only a trusted wireless network is configured and listed in Windows PNL. (By default, Windows Operating System will search for known SSIDs of a wireless network which has been connected previously. If an SSID matches the entries in Windows PNL, wireless connectivity will be established.)
2. Manage Windows PNL by deleting any unused wireless network in Windows PNL periodically.

6.1.5 Wireless Radio Interface

Wireless radio interface enable wireless clients to connect to a wireless network. Thus the interface needs to be handled appropriately.

The following tasks should be used as guidance in managing a wireless radio interface:

1. Only enable the wireless radio interface when the wireless client connects to a wireless LAN (i.e. always switch off after connecting to the wireless LAN).
2. Make connections only to trusted wireless clients (i.e. trusted wireless clients that are approved by the organisation) with a strong password.

6.2 ACCESS POINT PROTECTION

Wireless access points (APs) are specially configured nodes on wireless LANs. An access point acts as a central transmitter and receiver of wireless LAN radio signals. It is important to ensure that APs are protected from all kinds of wireless threats including tampering and theft.

Protecting APs should include, but is not limited to, configuration, positioning and signal coverage, SSID setting, encryption setting, AP management, MAC address filtering and radio frequency interface monitoring.

6.2.1 Configuration

APs need to be configured immediately upon deployment. This is to ensure that attackers do not know the default configuration such as the default manufacturer's password of an AP.

The following tasks should be used as guidance in configuring access points:

1. Immediately change the default configuration (i.e. factory setting configuration) of all APs that have been deployed. This includes:
   a) Service Set Identifier (SSID)
   b) Administrator credential
   c) Radio signal strength
   d) Remote web-based configuration portal
   e) IP service configuration
   f) Discovery protocol configuration

2. Change the default administrator's username and password of all APs in the web-based configuration portal. A strong password is one that consists of at least 10 characters and has a combination of upper and lowercase alphabets, numbers, signs and symbols. Please refer to http://www.esecurity.org.my for further details on how to create a strong password.
3. Different APs (if there is more than 1 AP in a wireless LAN) should have different passwords to connect to the web-based configuration portal.
4. Change passwords periodically in order to avoid using similar password for a long period of time.
5. Do not disclose passwords (if it not possible, limit the knowledge of the password to a group of trusted individuals who are aware of the impact of password disclosure).

6.2.2 Positioning and Signal Coverage

APs need to be physically placed appropriately in an organisation's premises. Thus it is essential for organisations to plan where to locate these APs to ensure they are not physically tampered with (e.g. stolen), and ensure that their signal strength is within the intended area.

The following tasks should be used as guidance when installing APs:

1. Conduct a full site survey to identify:
   a) APs placement and position
   b) Potential interference
   c) Coverage areas with specified signal strength
2. Identify all intended wireless coverage areas with specific signal strength for wireless services. Ensure signal strength/coverage of APs is based on the intended wireless coverage. This is to avoid signal leakage to outside boundaries of intended coverage such as on-the-street and neighbouring offices.
3. Ensure the optimum APs signal strength is within an intended coverage area. This is to prevent its signal leakage to an unauthorised user/attacker.
4. Search rogue (i.e. unauthorised) APs and displace them (if any) from the organisation's network. Most of the time, these rogue AP installations do not comply with organisational policies and procedures, which result in an open, non-secure entrance to the organisation's wireless network.
5. Change existing APs channel selection to non overlapping frequency in order to avoid interference.
6. Ensure that neighbouring access points are not using the same channel as the organisation's APs; otherwise use non-overlapping frequency to avoid interference.
7. Relocate APs to a better position through proper site survey if there is interference from electrical appliances i.e. microwave.
8. Ensure these APs are located in a secured area (so that they are not easily tampered or stolen).

6.2.3 Service Set Identifier (SSID) Setting

All APs need to use the same SSID in order to form communications to the wireless LAN. The SSID on wireless clients can be set manually by setting the SSID at the web-based configuration portal. SSIDs are case sensitive text strings which contain a sequence of alphanumeric characters.

The following tasks should be used as guidance when setting the SSID:

1. Ensure that the SSID setting for APs does not have descriptive information to avoid attackers from easily guessing and exploiting the organisation's SSID. Examples of information that should not be included in the SSID setting are:
   a) Name of organisations or departments
   b) Addresses, phone numbers or emails
   c) Default SSIDs
2. Disable the broadcasting of the SSID (configuration is done via web-based configuration portal).

6.2.4 Encryption

APs should be configured with encryption. This is to ensure that confidential data being transmitted over wireless networks are secure.

The following tasks should be used as guidance when configuring APs with strong encryption:

1. Configure APs with strong wireless encryption. Please refer to *Section 6.3 on Types of Wireless Encryption* for further information.
2. Consider replacing the APs if they do not support (or cannot support) the following wireless encryption: WPA/WPA2, WPA2-Enterprise with RADIUS. This is to ensure a higher level of security.

6.2.5 AP Management

Organisations should manage all APs which are installed in their wireless network. This is important so that the APs are protected, and their configuration setups should be reviewed periodically.

The following tasks should be used as guidance when managing APs in organisations:

1. Ensure that the web-based configuration portal for AP management uses strong authentication protocol (e.g. SSL and TLS).
2. Change administrator password for the web-based configuration portal periodically (refer to existing organisation's policy and procedure) or immediately if any AP theft has been reported.

6.2.6 Media Access Control (MAC) Address Filtering

The MAC address is a unique identifier for wireless APs. Most APs have a built-in feature called MAC address filtering. This feature is normally turned "off" by default (i.e because it requires some sort of configuration). It provides the ability to filter wireless clients and devices based on their MAC address from accessing the APs. Thus, to improve the security of wireless LANs, organisations should strongly consider enabling MAC address filtering; only devices with MAC addresses configured in the AP will be allowed to connect.

If MAC address filtering is being implemented within organisational wireless LANs, the following tasks should be used as guidance:

1. Enable MAC address filtering upon APs deployment.
2. Ensure that the MAC address filtering is not used in large wireless LANs (MAC address filtering is not recommended in large wireless network as it involves high maintenance of MAC addresses for all wireless clients).

6.2.7 Radio Frequency Interface Monitoring

Radio Frequency (RF) interface monitoring of APs for organisational wireless LAN is deployed through a wireless Intrusion Detection System (IDS) and wireless Intrusion Prevention System (IPS).

The following tasks should be used as guidance for RF interface monitoring:

1. Deploy RF interface monitoring through wireless IDS and IPS. These systems are intended to detect anomalous traffic and prevent any unusual frequency of attacks.
2. Ensure the IDS and IPS are periodically updated.

6.3 TYPES OF WIRELESS ENCRYPTION

Wireless encryption scrambles data on a wireless network so that only wireless clients that have a matching encryption key can read and understand the communications. The most vulnerable wireless network is when it is configured with no encryption. Therefore, organisations should not deploy APs without encryption as wireless data traffic can be viewed in plain-text format.

It is recommended that organisations implement sufficient security controls for wireless encryption that include, but are not limited to, Wired Equivalent Privacy (WEP), Wi-fi Protected Access (WPA/WPA2), and WPA2-Enterprise with RADIUS. These types of wireless encryption can be configured in the AP's web-based configuration portal.

6.3.1 Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) is an encryption algorithm built into the 802.11 standard to secure wireless networks. WEP encryption uses the RC4 stream cipher with 40 or 104 bit keys and a 24 bit initialisation vector [29]. It is, however, the weakest encryption security mechanism, as a number of flaws have been discovered in WEP encryption. WEP also does not have authentication protocol. Thus, it is recommended that organisations do not rely on WEP for security, and employ other security measures to protect their wireless network.

The following tasks should be used as guidance for organisations that implement WEP in their wireless LAN:

1. Change the WEP encryption setting to WPA/WPA2 with mutual authentication 802.1x protocols and EAP authentication methods.
2. Consider replacing the APs if they cannot support WPA/WPA2 encryption (for any reason).

6.3.2 Wi-fi Protected Access

Wi-fi protected access (WPA) and Wi-fi protected Access 2 (WPA2) encryption algorithms are created by Wi-Fi Alliance to secure wireless networks. The algorithms were created in response to several serious weaknesses found in WEP. WPA and WPA2 have two components (encryption and authentication) that are crucial to securing wireless LAN.

The following tasks should be used as guidance for organisations that implement WPA and WPA2 in their wireless LAN:

1. A password is required to connect to a wireless LAN when organisations implement WPA and WPA2. Use a very strong password that is made up of at least 10 characters and includes uppercase and lowercase letters as well as numbers and special characters.

6.3.3 WPA2-Enterprise with RADIUS

In order for organisations to use the most secure encryption for a wireless LAN, WPA2-Enterprise should be deployed. WPA2-Enterprise requires a RADIUS server. RADIUS is a networking protocol that provides centralised Authentication, Authorization, and Accounting (AAA) management for computers to connect to and use a network service [30].

If organisations decide to deploy WPA2-Enterprise with RADIUS in their wireless LAN, the following tasks should be used as guidance:

1. A password is required to connect to a wireless LAN when organisations implement WPA2-Enterprise with RADIUS. Use a very strong password that is at least 10 characters long and includes uppercase and lowercase letters as well as numbers and special characters.
2. Never use the same password for the RADIUS server that is used for the APs.

[29] http://www.tech-faq.com/wep-wired-equivalent-privacy.shtml
[30] http://www.wi-fiplanet.com/tutorials/article.php/3114511

7

OPERATIONAL CONTROLS

Operational controls in wireless LANs include protecting an organisation's premise, offices, labs and facilities, and people. These controls should be implemented together with management and technical controls.

The weakest link in a security chain is the human link; thus an organisation's employee security and security training program are addressed in this section. In addition, employees need to be informed on the correct procedures to report a wireless security incident. Patches and logs management are also being elaborated in this section as they are part of operational activities that organisations should implement. An inventory should be produced that lists all wireless equipments in organisations.

7.1 PHYSICAL AND ENVIRONMENTAL PROTECTION

Physical and environmental protection provides measures to prevent unauthorised physical access, damage and interference to an organisation's premises and information security [31]. In wireless security, it is the most fundamental step for ensuring that only authorised users have access to wireless facilities and equipment. For example, photo identification, card badge readers, or biometric devices can be used to minimise the risk of authorised access to the building or facilities that house wireless LAN equipment.

The following tasks should be used as guidance in physical and environmental protection:

1. Produce physical and environmental security policies and procedures.
2. Ensure that policies and procedures are approved and endorsed by senior management.
3. Define clearly the organisation's physical security perimeter, entry control, secure working areas, public access areas, delivery and loading areas, as well as wireless equipment security that includes the equipment's location, cabling and supporting utilities.
4. Monitor periodically and retain logs related to physical security controls such as CCTV footage and server room access logs for a period of time (in accordance to organisational policies, procedures and/or security requirements).

7.2 HUMAN RESOURCES SECURITY

Human resources security provides roles and responsibilities of employees, contractors and third party users (i.e. external users who have access to organisational resources), as defined and documented in accordance with the organisational information security policy [32]. It is important to ensure that the human resources element is secure as most wireless security incidents are breached by internal employees.

The following tasks should be used as guidance in ensuring human resources security:

1. Define and document the security roles and responsibilities of its employees, contractors and third party users in accordance with an organisation's policies and procedures.
2. Carry out background verification checks, screening, and vetting procedures in accordance with relevant laws and regulations upon hiring new employees, contractors and third party users.

[31] ISO/IEC 27001:2005 Information Security Management Systems
[32] ISO/IEC 27001:2005 Information Security Management Systems

3. Produce terms and conditions of employment that states the employees, contractors and third party users' responsibilities for the organisation's wireless network. They shall agree and sign the terms and conditions of their employment contract prior to reporting to work.
4. Ensure that termination procedures include responsibilities of employees, contractors and third party users to return all their wireless devices, and removal of their access rights from wireless networks, systems and applications.

7.3 TRAINING AND AWARENESS PROGRAMME

A training and security awareness program is a fast and effective platform to inform employees and enhance their knowledge on wireless network security. The awareness program should provide detailed explanation of wireless LAN security so that employees are fully aware of its importance and what is expected of them.

If employees were not communicated on what to expect from them and what management considers unacceptable behaviour, an organisation will have a much harder time enforcing rules, and may be held liable for security issues caused by the employees.

The following tasks should be used as guidance in planning and conducting a training and awareness program:

1. Develop a security training and awareness program that is suitable for the identified audience (i.e. employees, contractors and third party users).
2. Conduct appropriate awareness training on wireless networks and provide regular updates in organisational policies and procedures to employees, contractors and third party users.

7.4 INCIDENT HANDLING MANAGEMENT

A wireless network security incident is made up of one or more unwanted or unexpected wireless security events [33]. It happens when an identified occurrence of a wireless system, service, or network indicates a possible breach of policy or failure of safeguards, or even an unknown situation that may be security relevant. It can compromise the security of an organisation's wireless network and weaken or impair its business operations. Organisations should ensure these security incidents are handled in a timely manner, allowing corrective action to be taken.

The following tasks should be used as guidance in handling incidents related to wireless network security:

1. Provide guidelines on reporting procedures for theft of wireless devices and security incidents related to it.
2. Ensure that wireless network security incidents are reported through a dedicated and appropriate channel immediately.
3. Provide mechanisms to monitor and quantify the types, volumes, etc. of wireless network security incidents.
4. Collect, retain and preserve any evidence with regards to wireless network security incidents especially those related to legal action.

7.5 PATCH MANAGEMENT

Organisations should implement appropriate patch management mechanisms for prompt updates of their wireless devices and software applications. Authorised personnel should apply patches and security enhancements for wireless equipments whenever updates are available and published by the vendor. CISO (please refer to *Section 5.1 Roles and Responsibilities*) is responsible to oversee and regularly monitor the applied patches and security enhancements done by the authorised personnel.

[33] ISO/IEC 27002:2005 Information Security Management Systems

The following tasks should be used as guidance in patch management for wireless devices and related software:

1. Identify relevant patches to be implemented in each wireless equipment and/or software.
2. Identify and produce roles and responsibilities of authorised personnel to perform patches and security enhancements.
3. Ensure patches and security enhancements are completed in a reliable and timely manner and monitored by CISO.
4. Provide validation checks and procedures to assess the implementation of patches and security enhancements.

7.6 WIRELESS EQUIPMENT INVENTORY

Organisations should keep an inventory of their wireless equipments such as wireless devices and hardware. This inventory is important as organisations will be able to keep track of lost or stolen hardware since passwords may be recovered from hardware. Immediate change of password might be needed.

The following tasks should be used as guidance for organisations in doing a wireless equipment inventory:

1. Ensure all wireless equipments and configurations are recorded.
2. Inventory should be reviewed periodically to ensure they tally with the current numbers of wireless devices and hardware.
3. Change all passwords of APs in the web-based configuration portal immediately in the event of theft.

Appendix A

Security Controls Checklist

The table below provides a checklist of three security controls: Management, Technical, and Operational, as described earlier in the Guideline. This checklist should be used by organisations to secure their wireless LAN.

SECTION	SECURITY CONTROLS	YES	NO	REMARKS
5	**Management Controls**			
5.1	**Roles and Responsibilities**			
1.	Support and commitment from senior management for planning and implementing security for wireless LANs is demonstrated clearly.			
2.	Risk assessment is approved by senior management before implementing wireless LAN technology.			
3.	Relevant policies and procedures related to wireless LAN security are developed, endorsed and communicated to employees.			
4.	Dedicated CISO is employed to oversee the wireless network security.			
5.	Roles and responsibilities related to protection of wireless devices are clearly defined.			
6.	Training and awareness sessions are attended by all employees to understand technical and security implications of wireless technologies.			
5.2	**Policies and Procedures**			
1.	Policies and procedures related to wireless LAN security are developed and endorsed by senior management.			
2.	Awareness and dissemination of policies and procedures to all employees are sufficient.			
3.	Policies and procedures are reviewed periodically or at planned intervals.			
5.3	**Risk Assessment**			
1.	Scope, methodology and strategy for risk assessment on wireless LANs are defined.			
2.	Risk assessment is performed based on the defined scope which should include these:			
3.	Existing policies and procedures .			
4.	Location of access points.			
5.	Types of wireless transaction.			
6.	Wireless LAN users.			
7.	Dependency on wireless LAN infrastructure.			

SECTION	SECURITY CONTROLS	YES	NO	REMARKS
5.4	**Wireless Network Assessment**			
1.	Security requirements for wireless network assessment are produced.			
2.	Objective, scope and frequency of wireless network assessment is produced.			
3.	Roles and responsibilities for wireless network assessment are defined.			
4.	Wireless network assessment is performed after approval from senior management.			
6	**Technical Controls**			
6.1	**Wireless Client Protection**			
6.1.1	***Encryption***			
1.	Encryption software is used to encrypt wireless data traffic at application layer.			
6.1.2	***Malicious Code Protection***			
1.	Malicious code protection software is installed at wireless clients.			
2.	Malicious code protection software is configured (upon installation) to be updated automatically.			
3.	Full scan is scheduled periodically at the wireless clients during low activity.			
6.1.3	***Personal Firewall Protection***			
1.	Personal firewall is installed at wireless clients.			
2.	Personal firewall software is configured (upon installation) to be updated automatically.			
6.1.4	***Windows PNL***			
1.	Only trusted and desired wireless networks are configured and listed in Windows PNL.			
2.	Unused entries in Windows PNL are deleted and reviewed periodically.			
6.1.5	***Wireless Radio Interface***			
1.	Wireless radio interface is turned ‘on’ only when the wireless client connects to a wireless LAN.			
2.	Ensure connections to trusted wireless clients only.			
6.2	**Access Point Protection**			
6.2.1	***Configuration***			
1.	Default configuration of deployed access points has been changed. This includes:			
2.	SSID.			
3.	Administrator credential.			

SECTION	SECURITY CONTROLS	YES	NO	REMARKS
4.	Radio signal strength.			
5.	Remote web access management.			
6.	IP service configuration.			
7.	Discovery protocol configuration.			
8.	Default administrative password has been changed to a stronger password.			
6.2.2	***Positioning & Signal Coverage***			
1.	Site survey has been conducted to identify the following:			
2.	AP placement and position.			
3.	Potential interference.			
4.	Coverage areas with specified signal strength.			
5.	Intended wireless coverage areas with specific signal strength are identified.			
6.	Signal strength is within intended coverage area.			
7.	Rogue access points are searched and removed.			
8.	Access point's channel selection is changed to non overlapping frequency.			
9.	Neighbouring access point is not using the same channel.			
10.	Access point is relocated to a better position via proper site surveys.			
6.2.3	***SSID Setting***			
1.	SSID setting for APs is not configured with too descriptive information (e.g. organisation name, address, email, etc).			
2.	SSID broadcasting is disabled.			
6.2.4	***Encryption***			
1.	APs are configured with strong encryption.			
2.	APs are replaced if it does not support the following wireless encryption: WPA/WPA2, WPA2-Enterprise with RADIUS.			
6.2.5	***AP Management***			
1.	Strong authentication protocol (e.g. SSL and TLS) is used for Web-based configuration portal management for AP management.			
2.	Unused management port is turned off.			
3.	Administrator password for web-based configuration portal is changed periodically (or immediately if access point theft has been reported).			

SECTION	SECURITY CONTROLS	YES	NO	REMARKS
6.2.6	***MAC Address Filtering***			
1.	MAC address filtering is enabled upon AP deployment.			
2.	MAC address filtering is not used in large wireless LANs.			
6.2.7	***Radio Frequency Interface Monitoring***			
1.	RF interface monitoring is deployed through wireless IDS and IPS.			
2.	IDS and IPS are periodically updated.			
6.3	**Wireless Encryption**			
6.3.1	***WEP***			
1.	Access point with WEP encryption is changed to WPA/WPA2 with 802.1x protocol or EAP authentication methods.			
2.	Access point is replaced if it does not (and cannot) support WPA/WPA2 encryption.			
6.3.2	***WPA/WPA2***			
1.	Password created is longer than 20 characters and includes uppercase and lowercase letters as well as numbers and special characters.			
2.	Password is periodically changed (immediately if hardware theft had been reported).			
3.	Password is not disclosed.			
6.3.3	***WPA2-Enterprise with RADIUS Authentication***			
1.	Password created is longer than 16 characters.			
2.	Different RADIUS password is used for different APs.			
7	**Operational Controls**			
7.1	**Physical and Environmental Protection**			
1.	Policies and procedures related to physical and environmental security are produced.			
2.	Policies and procedures are approved and communicated to all employees.			
3.	Physical security (premise perimeter, entry control, etc) and wireless equipment security is secured according to policies and procedures.			
4.	Logs (CCTV footage, server room, etc) are monitored periodically and retained.			

SECTION	SECURITY CONTROLS	YES	NO	REMARKS
7.2	**Human Resources Security**			
1.	Roles and responsibilities related to wireless LAN security are defined and documented.			
2.	Background verification, screening, and vetting of employees is carried out.			
3.	Terms and conditions of employment for employees are produced.			
4.	Termination procedures (return wireless devices, access rights removal) are produced.			
7.3	**Training & Awareness Program**			
1.	Training and awareness program on wireless LAN security is developed for identified audience.			
2.	Security training and awareness program is conducted periodically.			
6.4	**Incident Handling Management**			
1.	Procedure for reporting loss of wireless devices is produced.			
2.	Wireless network security incident is reported promptly.			
3.	Mechanism to monitor and quantify wireless network security incident is produced.			
4.	Evidence related to wireless network security incident is collected, retained and preserved.			
6.5	**Patch Management**			
1.	Patches and security enhancement for wireless devices are identified.			
2.	Patches and security enhancement are performed by authorised personnel.			
3.	Patches for wireless devices are implemented/deployed in timely manner.			
4.	Implementation of patches and security enhancements is validated.			
5.5	**Wireless Equipment Inventory**			
1.	All wireless equipments and configurations are documented and recorded.			
2.	Inventory is reviewed periodically.			
3.	Passwords for APs in web-based management portal are immediately changed in the event of theft.			

Table 1: Checklist for Security Controls in Wireless LAN

Appendix B

IEEE 802.11 Standard

The table below summarises the various aspects of IEEE 802.11 standards. The table contains a description, remarks, and estimated product availability for each standard. This table was taken from NIST SP800-48 Revision 1: Guide to Securing Legacy IEEE 802.11 Wireless Networks [34].

NO	IEEE STANDARD	DESCRIPTION	REMARKS	AVAILABILITY
1	**802.11a**	A physical layer standard that operates in the 5 GHz UNII radio band. It specifies eight available radio channels. (In some countries, 12 channels are permitted.) The maximum link rate is 54 Mbps per channel; maximum actual user data throughput is approximately half of that, and the throughput is shared by all users of the same radio channel. The data rate decreases as the distance between the user and the AP increases.	**Higher performance** In most office environments, the data throughput will be greater than for IEEE 802.11b. In addition, the greater number of non-overlapping radio channels (eight as opposed to three) provides better protection against possible interference from neighboring APs.	This standard was completed in 1999. Products are available now.
2	**802.11b**	This is a physical layer standard in the 2.4 GHz ISM radio band. Maximum link rate is 11 Mbps per channel, but maximum user throughput will be approximately half of this because the throughput is shared by all users of the same radio channel. The data rate decreases as the distance between the user and the AP increases.	**Performance** Installations may suffer from speed restrictions in the future, as the number of active users increase, and the limit of three non-overlapping channels may cause interference from neighboring APs.	This standard was completed in 1999. A wide variety of products has been available since 2001.

34 NIST SP 800-48r1 Guide to Securing Legacy IEEE 802.11 Wireless Networks

NO	IEEE STANDARD	DESCRIPTION	REMARKS	AVAILABILITY
3	**802.11d**	This standard is supplementary to the MAC layer in IEEE 802.11 to promote worldwide use of IEEE 802.11 WLAN. It will allow APs to communicate information on the permissible radio channels with acceptable power levels for user devices. The IEEE 802.11 standards cannot legally operate in some countries; the purpose of 802.11d is to add features and restrictions to allow WLANs to operate within the rules of these countries.	**Promote worldwide use** In countries where the physical layer radio requirements are different from those in North America, the use of WLANs is lagging behind. Equipment manufacturers do not want to produce a wide variety of country-specific products, and users that travel do not want a bag full of country-specific WLAN PC cards. The outcome will be country-specific firmware solutions.	This standard was completed in 2001. Products are available now.
4	**802.11e**	This standard is supplementary to the MAC layer to provide QoS support for WLAN applications. It will apply to IEEE 802.11 physical standards a, b, and g. The purpose is to provide classes of service with managed levels of QoS for data, voice, and video applications.	**Quality of service** This standard provides some useful features for differentiating data traffic streams. It is essential for future audio and video distribution.	This standard was completed in 2005. Products are available now.
5	**802.11f**	This is a "recommended practice" document that aims to achieve AP interoperability within a multi-vendor WLAN. The standard defines the registration of APs within a network and the interchange of information between APs when a user is handed over from one AP to another.	**Interoperability** This standard will work to increase vendor interoperability, reduce vendor lock-in, and allow multi-vendor infrastructures.	This recommend-ed practice was completed in 2003. Products are available now.

NO	IEEE STANDARD	DESCRIPTION	REMARKS	AVAILABILITY
6	**802.11g**	This is a physical layer standard for WLANs in the 2.4 GHz ISM radio band. The maximum link rate is 54 Mbps per channel whereas IEEE 802.11b offers 11 Mbps. The IEEE 802.11g standard uses orthogonal frequency-division multiplexing (OFDM) modulation but for backward compatibility with IEEE 802.11b, it also supports complementary code-keying (CCK) modulation and, as an option for faster link rates, allows packet binary convolutional coding (PBCC) modulation.	**Higher performance with IEEE 802.11b backward compatibility** This standard provides speeds similar to IEEE 802.11a and backward compatibility with IEEE 802.11b.	This standard was completed in 2003. Products are available now.
7	**802.11h**	This standard is supplementary to the MAC layer to comply with European regulations for 5 GHz WLANs. European radio regulations for the 5 GHz band require products to have transmission power control (TPC) and dynamic frequency selection (DFS). TPC limits the transmitted power to the minimum needed to reach the farthest user. DFS selects the radio channel at the access point to minimize interference with other systems, particularly radar.	**European regulation compliance** This is necessary for products to operate in Europe. Completion of IEEE 802.11h provides better acceptability within Europe for IEEE-compliant 5 GHz WLAN products. A group that is rapidly dwindling will continue to support the alternative HyperLAN standard defined by the European Telecommunicati-ons Standard Institute (ETSI).	This standard was completed in 2003. Products are available now.

NO	IEEE STANDARD	DESCRIPTION	REMARKS	AVAILABILITY
8	**802.11i**	This standard is supplementary to the MAC layer to improve security. It applies to IEEE 802.11 physical standards a, b, and g. It provides improved security over Wired Equivalent Privacy (WEP) with new encryption methods and authentication procedures. IEEE 802.1X forms a key part of IEEE 802.11i.	**Improved security** The IEEE 802.11i amendment defines two data confidentiality and integrity protocols for Robust Security Network Associations (RSNA): TKIP and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), using AES. Federal agencies are required to use FIPS-validated cryptographic modules.32 NIST SP 800-97 contains specific recommendations and guidance for IEEE 802.11i.	This standard was completed in 2004. Products are available now.
9	**802.11k**	This standard defines Radio Resource Measurement enhancements to provide management and maintenance interfaces to higher layers for mobile WLANs.	**Resource radio management** This standard will enable seamless Basic Service Set (BSS) transitions between WLANs through the discovery of the best available AP and improve network traffic by distributing users to under-used APs.	Draft 11 was approved in January 2008. Final ratification has not yet occurred.
10	**802.11m**	This is a supplementary maintenance standard to the IEEE 802.11-1999 (reaff. 2003) standard.	**Editorial maintenance** This initiative is to perform editorial maintenance, corrections, improvements, clarifications, and interpretations to the IEEE 802.11-1999 (reaff. 2003) Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications standard.	This standard was completed and is part of 802.11-2007.
11	**802.11n**	This standard investigated the possibility of improving the IEEE 802.11 standard to provide high throughput at a theoretical 300 Mbps.	**Increased data throughput** The purpose of this standard is to improve the IEEE 802.11 WLAN user experience by providing significantly higher throughput using MIMO antennas and receivers and different coding schemes.	This standard is expected to be completed in 2009.

NO	IEEE STANDARD	DESCRIPTION	REMARKS	AVAILABILITY
12	802.11p	This standard is an amendment of IEEE 802.11 to support communication between vehicles and the roadside, and between vehicles while operating at speeds up to a minimum of 200 kilometers/hour for communication ranges up to 1,000 meters. The amendment will support communications in the 5 GHz bands—specifically 5.850–5.925 GHz band within North America, with the aim to enhance the mobility and safety of all forms of surface transportation, including rail and marine. Amendments to the Physical (PHY) and MAC layers will be limited to those required to support communications under these operating environments within the 5 GHz bands. This standard is also referred to as the Wireless Access for Vehicular Environment (WAVE).	**Wireless access for vehicles** This standard amends the existing IEEE 802.11 standard to make it suitable for interoperable communications to and between vehicles. The primary reasons for this amendment include the unique transport environments and the very short latencies required (some applications must complete multiple data exchanges within 4 to 50 milliseconds).	This standard is scheduled to be completed in April 2009.
13	802.11r	This standard is supplementary to the IEEE 802.11 Medium Access Control (MAC) layer standards and creates improvements to minimise or eliminate the amount of time data connectivity between the Station (STA) and the Distribution System (DS) during a BSS transition.	**Fast BSS transitions** This standard improves BSS handoffs within IEEE 802.11 networks. This is a critical component to support real-time constraints imposed by applications such as Voice over Internet Protocol (VoIP).	This standard is scheduled to be published in mid-2008.

NO	IEEE STANDARD	DESCRIPTION	REMARKS	AVAILABILITY
14	**802.11s**	This standard defined the IEEE 802.11 ESS Mesh with an IEEE 802.11 Wireless Distribution System (WDS) using the IEEE 802.11 MAC/PHY layers that support both broadcast/ multicast and unicast delivery over self-configuring multi-hop topologies.	**ESS mesh networking** This standard provides a protocol for auto-configuring paths between APs over self-configuring multi-hop topologies in a WDS to support both broadcast/ multica-st and unicast traffic in an ESS Mesh using the four-address frame format or an extension.	This standard is scheduled to be completed in 2008.
15	**802.11t**	This is a "recommended practice" and will provide a set of performance metrics, measurement methodologies, and test conditions to enable measuring and predicting the performance of IEEE 802.11 WLAN devices and networks at the component and application level as a recommended practice.	**Wireless performance protection** This standard enables testing, comparison, and deployment planning of IEEE 802.11 WLAN products so that performance and product specifications can be captured through a common and accepted set of performance metrics, measurement methodologies and test conditions.	This recommended practice is scheduled to be completed in 2008.
16	**802.11u**	This standard is an amendment to the IEEE 802.11 MAC and PHY layers to support InterWorking with External Networks.	**Internetworking with external networks** This will provide amendments to the IEEE 802.11 PHY/MAC layers, which will enable InterWorking with other networks and granting of limited access, based on a relationship with an external network. This includes both enhanced protocol exchanges across the air interface and provision of primitives to support required interactions with higher layers for InterWorking.	This standard is in the proposal evaluation stage and a scheduled completion date has not been set.

NO	IEEE STANDARD	DESCRIPTION	REMARKS	AVAILABILITY
17	**802.11v**	This standard will create amendments to provide Wireless Network Management enhancements to the IEEE 802.11 MAC, and PHY layers to allow configuration of client devices connected to the network.	**Wireless network management** This will provide amendments to the IEEE 802.11 PHY/MAC layers that enable management of attached stations in a centralised or a distributed fashion (e.g., monitoring, configuring, and updating) through a layer mechanism. Although the IEEE 802.11k Task Group is defining messages to retrieve information from the station, the ability to configure the station is not within its scope. The proposed Task Group will also create an Access Port Management Information Base (AP MIB).	This standard is in the early proposal stages and a scheduled completion date has not been set.
18	**802.11w**	This standard will enhance IEEE 802.11 MAC layer security for selected management frames by providing data integrity, data origin authenticity, replay protection, data confidentiality, and other security features.	**Management frame protection** This will extend the use of IEEE 802.11i to selected management frames to increase the overall security of IEEE 802.11-based networks. The increased level of security is intended to mitigate malicious network-based attacks, such as DoS attacks. In addition, this amendment will provide security for sensitive network information that will be included in transmissions outlined in several new amendments, including IEEE 802.11r, IEEE 802.11k, and IEEE 802.11y.	The standard is under development and is expected to be completed and ratified in 2008.

Table 2: Summary of IEEE 802.11 standards

References

[1] *ISO/IEC 27001:2005, Information Technology – Security Techniques – Information Security Management Systems,* First Edition 2005-10-14.

[2] *ISO/IEC 27002:2005, Information Technology – Security Techniques – Code of Practice for Information Security Management,* First Edition 2005-06-15.

[3] *Ross, Johnson, Katzke et all. NIST Special Publication 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans",* Third Public Draft, June 2007.
http://csrc.nist.gov/publications/drafts/800-53A/draft-SP800-53A-fpd-sz.pdf

[4] Karygiannis,Tom and Owens, Les. *NIST Special Publication 800-48, "Wireless Network Security: 802.11, Bluetooth and Handheld Devices",* First Edition, November 2002.
http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf.

[5] Scarfone, Dicoi, Sexton, Tibbs*. NIST Special Publication 800-48, Revision 1, "Guide to Securing Legacy IEEE 802.11 Wireless Networks",* July 2008.
http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf

[6] Check Point Software Technologies Ltd, *Building Secure Wireless LANs, 2004.*
http://www.virtual.com/whitepapers/Check_Point_Building_Secure_Wireless_LANs_wp.pdf, 11/02/2008.

[7] AirDefense,Inc, *Wireless LANs: Risks and Defenses,* 2002.
http://www.itsec.gov.cn/webportal/download/73.pdf, 11/02/2008.

[8] Symantec Enterprise Security, *Wireless LAN Security-Enabling and Protecting the Enterprise.*
http://www.symantec.com/avcenter/reference/symantec.wlan.security.pdf, 11/02/2008.

[9] Glenn, Josh. *WLAN Security Challenges,* 08/03/2005.
http://www.securitydocs.com/library/3534, 11/02/2008.

[10] *Wireless LAN Policy.*
http://www.sans.org/resources/policies/Wireless_Communication_Policy.pdf, 11/02/2008.

[11] *802.11 Security Series: The Temporal Key Integrity Protocol.*
http://www.menet.umn.edu/~akash/links/80211_part2.pdf, 11/02/2008.

[12] *Weakness in Passphrase Choice in WPA Interface.*
http://wifinetnews.com/archives/002452.html, 11/02/2008.

[13] *LEAP Recommendation from Cisco Product Security Incident Response Team.*
http://asleap.sourceforge.net/README, 11/02/2008.

[14] *Wireless LAN Security, 802.11/Wireless LAN Wardriving & Warchalking.*
http://www.wardrive.net, 11/02/2008.

[15] Flickenger, Roger Weeks. *Wireless Hacks,* 2nd Edition, O'Reilly, 2005.

[16] Moerschel, Dreger, Tom Carpenter. *CWSP Certified Wireless Security Professional, 2nd Edition,* Grant McGraw Hill, 2006.

[17] *Security controls for Operational Risk Management.* http://www.occ.treas.gov/ftp/release/2003-53c.pdf, 05/05/2008.

[18] Kipper, Grogery. *Wireless Crime and Forensic Investigation.* Auerbach Publications, Taylor & Francis Group. 2007.

[19] Mell, Kent, Nusbaum, Joseph. *NIST Special Publication 800-83, "Guide to Malware Incident Prevention and Handling",* November 2005. http://csrc.nist.gov/publications/nistpubs/ 800-83/SP800-83.pdf

[20] Ross, Katzke, Johnson et all. *NIST Special Publication 800-53 Revision 1, "Recommended Security Controls for Federal Information Systems",* December 2006. http://csrc.nist.gov/publications/nistpubs/ 800-53-Rev1/800-53-rev1-final-clean-sz.pdf

CyberSecurity Malaysia
Block A, Level 8, Mines Waterfront Business Park
No. 3, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia
Tel : +603 - 8992 6888 Fax : +603 - 8945 3205
E-mail : info@cybersecurity.my
www.cybersecurity.my

Ministry of Science, Technology and Innovation

Best Brand Internet Security

CERTIFIED TO ISO/IEC 27001:2005
CERT NO.: AR4636