



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"  
at <http://www.giac.org/registration/gsec>

GIAC Security Essentials Certification (GSEC)  
Practical Assignment version 1.4b  
Submitted by: Keng Hoe LIM  
27 August 2003

# **Security Guidelines for Wireless LAN Implementation**

© SANS Institute 2003, Author retains full rights.

## **ABSTRACT**

The emergence of IEEE 802.11 standards has significantly contributed to the popularity of Wireless Local Area Network (WLAN) implementations over recent years in business organizations, government bodies and even home environment. While WLAN provides greater mobility and flexibility, it also poses security risks that must not be overlooked.

This paper focuses on the security issues of WLAN and attempts to put in place a set of security guidelines to help organizations and home users in securing their WLANs.

© SANS Institute 2003, Author retains full rights.

## INTRODUCTION

A Wireless LAN (WLAN) is a local area network without physical interconnecting wires. The computing devices in a WLAN communicate with one another using radio frequency electromagnetic airwaves.

A typical WLAN implementation is depicted in the pictorial representations in *Annex A*<sup>1</sup>. A WLAN can be configured in 2 modes, namely the *ad-hoc* or the *infrastructure* network mode. An *ad-hoc* WLAN allows wireless stations to connect directly to one another for sharing of files or resources. In an *infrastructure* WLAN, wireless stations communicate with one another via the access point, which also serves as the bridge that interconnects the WLAN and the wired network.

Various WLAN standards or specifications, such as IEEE 802.11a, IEEE 802.11b, OpenAir, HiperLAN, Bluetooth and HomeRF exist today. Among these standards, IEEE 802.11b is the most widely used in WLAN products.

Businesses, government and home users are increasingly deploying WLAN for mobility. It is gaining popularity as a viable alternative to replace or extend the traditional wired implementation. A summary of the various 802.11 standards is in *Annex B* [3].

While WLAN provides greater mobility and flexibility, it also poses several security risks that are not faced in a wired network. Unlike the wired network, the perpetrator does not need physical access to the WLAN, as the medium is shared radio frequency. In addition, the current WLAN security mechanisms used to ensure proper access control and confidentiality of wireless communication are inadequate<sup>2</sup>. The Service Set Identifier (SSID) used in controlling access to the WLAN is usually broadcast in clear or can be derived easily; the Wired Equivalent Privacy (WEP) used to encrypt the wireless transmission can also be discovered in a short period of time.

With increasing deployments of WLAN and the interdependencies of organisations' infrastructure and networks, it is essential to ensure that the deployment of WLAN will not compromise the confidentiality, integrity and availability of information and operations.

## OBJECTIVE

This document provides security guidance on the implementation of WLAN for both office and home environments. Organisations would need to assess their

---

<sup>1</sup> Icons adapted from [3].

<sup>2</sup> Wired Equivalent privacy (**WEP**) and Service Set Identifier (**SSID**) are the two security mechanisms in IEEE 802.11b for providing confidentiality and access control. Researchers found severe shortcoming in WEP where the secret key used in encryption can be discovered in a short period of time. SSID that is used as an access control mechanism in accessing WLAN are usually broadcast in clear or can be derived easily. Hence, the WLAN industry is looking towards the new IEEE 802.11i standard, which is currently still in draft, as a long-term solution for WLAN security. The IEEE 802.11i standard attempts to address security in WLAN.

specific security needs in the implementation of WLAN and determine if the guidelines are applicable to their environment.

The guidelines should be used in conjunction with the organisation's security policies, standards and guidelines, in particular the sections on client and network security.

## SCOPE

The security guidelines cover the following areas:

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 and
10. Logging and Audit Trails

## SECURITY THREATS

The security risks in WLAN extend beyond those in a wired network to include the new risks introduced by the weaknesses in wireless protocols. The security threats posed by WLAN include:

Eavesdropping – Intercepting information that is transmitted over the WLAN is generally easier as it can be done from a distance up to kilometres<sup>3</sup> outside of the building perimeter without any physical network connection required. The information intercepted can be read if transmitted in clear or easily deciphered if only WEP encryption is used.

Traffic analysis – The perpetrator gains intelligence by monitoring the transmissions for patterns of communication, information flow between communicating parties and deciphering of encrypted traffic captured. This may result in disclosure of sensitive information.

Data Tampering – The information transmitted over the WLAN can be deleted, replayed or modified by the perpetrator via man-in-the-middle attack<sup>4</sup>. This may result in a loss of data integrity and availability.

---

<sup>3</sup> With high gain antennas, the distance can vary up to kilometres even when the nominal or claimed operating range of wireless device is less than a hundred meters. An antenna with 24dBi gain can reach as far as 32 miles and it is widely available via the Internet.

<sup>4</sup> Using devices to masquerade as a trusted wireless access point, the perpetrator can manipulate all wireless traffic transmission between the wireless client and the backend systems.

**Masquerading** – The perpetrator gains unauthorized access to the information and network resources within the WLAN or other interconnected network by impersonating the identity of an authorised WLAN user. The perpetrator can create further havoc by launching attacks or introducing malicious codes that will disrupt operations.

**Denial of Service (DoS)** – The perpetrator 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 perpetrator can cause denial of service without close proximity to the targeted WLAN. Furthermore, it is not possible to locate the perpetrator base on current detection solutions. This attack can cause a denial of service and unavailability of information and network resources.

**Wireless Clients Attacks** – The perpetrator 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.

## **SECURITY GUIDELINES**

The following is a set of general security guidelines that would offer ample security in a normal day-to-day implementation. However, organisations should exercise discretions in ascertaining the feasibility of such implementations and if necessary, put in appropriate or equivalent measures to mitigate any security risks.

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.

A pictorial summary of my recommendations for both office and home environment is depicted in *Annex C*<sup>5</sup>.

### **Physical Security**

The wireless station and its WLAN adaptor card should not be physically exposed to prevent theft and unauthorised access to the WLAN.

The access points should be placed within the physically protected office environment to prevent them from any unauthorised access and physical

---

<sup>5</sup> Icons adapted from [3].

tampering. Security alarm system can also be used wherever applicable.

The access points should be physically located away from external sources of electromagnetic interference, e.g. microwave ovens. 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.

A site review should be conducted to assess the coverage of WLAN to minimise 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.

### **Confidentiality and Integrity**

Confidential or important information should not be transmitted unprotected over the WLAN. The information should be encrypted prior to transmission over the WLAN so as to protect its confidentiality and integrity. Due to its vulnerabilities [2], the 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. Wherever possible, 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.

### **Key Management**

The symmetric encryption keys, e.g. the WEP keys stored in the access points and wireless stations, should be protected from unauthorised access. This is to prevent any unauthorised personnel from decrypting the WLAN data traffic if he gets hold of the symmetric encryption keys.

Strong symmetric encryption, e.g. using 128-bit key length, should be used to protect the information that is transmitted over the WLAN. The encryption keys should be changed periodically, e.g. once every 90 days.

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.

The symmetric encryption keys should be protected during key distribution to the users. The new keys should be sent to the users either in encrypted form or through other secure means to prevent unauthorised access to the keys during transit.

Wherever possible, the symmetric encryption keys should be loaded directly into the access point without traversing any intermediary networks which

could be sniffed by unauthorised personnel. 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.

### **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 authorised wireless stations but not the users. As such, unauthorised 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 unauthorised access to the organisation's internal network via the WLAN.

### **Access Control**

The access point should be configured to allow only authorised wireless stations to associate with the WLAN. Only authorised wireless stations, which have the same network name or Extended Service Set ID (ESSID), authorised Media Access Control (MAC) address and WEP Shared Key, should be allowed to access the WLAN.

The access point should be configured to drop any unencrypted network traffic so that unauthorised wireless stations or rogue access points cannot associate with the access point if they do not know the shared secret, e.g. the WEP key.

Existing network or application level access control and user authentication should be maintained to prevent unauthorised access to the internal wired network and applications in the event that the security of the WLAN has been compromised.

Access control mechanisms such as firewalls should be implemented to segregate the WLAN from the internal wired network. The WLAN should be deployed in a different network segment, which is separate from the internal wired network. Network or IP filtering can be implemented at the gateway to ensure that only authorised network traffic from the WLAN or legitimate access points are allowed to enter the wired network. This is to prevent unauthorised access to the internal wired network via rogue access points.

### **Client security**

Access control and intrusion detection mechanisms should be installed on the wireless station where possible to prevent and detect any unauthorised access to the wireless station over the WLAN.

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 minimise set-up of rogue access points. This is to prevent unauthorised access to the internal wired network via the rogue access point due to insecure configurations (e.g. WEP not enabled, no MAC address control list).

The wireless station should not be configured for network file sharing without any protection to prevent any unauthorised access to his local files.

### **User Awareness**

Where it is not required, the 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. This is to prevent unauthorised access to the user's files if they are not protected.

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. This will reduce the risk of attacks on the wireless station over the WLAN.

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. This is to prevent any unauthorised access to the internal wired network via the wireless station.

### **Administration of access points**

The access to WLAN key distribution program should be controlled and limited to the administrators only.

The built-in COM ports of the access point should be disabled or password-protected to prevent any unauthorised access to the access points.

All unnecessary services and ports in the access points should be removed or closed.

The default Service Set ID (SSID) of each access point should be changed. This is to prevent any wireless clients from connecting to the access point. If possible, SSID should not be broadcasted.

The default SNMP community string should be changed if the access point has SNMP agent running on it. This is to prevent an attacker from reading or writing to the access point.

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. This might allow the attacker to monitor the broadcasted data, which may not be intended for all the wireless clients.

Firewall and VPN can be used to mitigate these risks by segregating the wired/wireless networks and encrypting the data packets [4].

Periodic scanning on the WLAN should be conducted to detect the presence of rogue access points, unauthorised ports/services or any security vulnerabilities in the network.

The password for remote management of access points can be captured and used to gain unauthorised 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.

The user should be required to report the loss of his wireless station and WLAN adaptor card immediately so that prompt action can be taken to prevent any unauthorised access via the lost wireless equipment, e.g. the MAC address of the user's WLAN adaptor card can be revoked immediately.

The WLAN adaptor card should be returned to the organisation upon staff resignation or termination to prevent the user from gaining unauthorised access to the WLAN.

The users should not be allowed to install or run any network sniffer on their PCs without first seeking appropriate approval. The use of authorised network sniffer should be logged and accounted for to prevent any misuse.

### **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 organisation's 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.

### **Logging and Audit Trails**

Unauthorised network traffic and access to the WLAN should be logged, e.g. using Intrusion Detection System, to detect attacks directed over the WLAN. Any exceptions or abnormal network activities should be logged and alerts sent to the administrators, as per the organisation's 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.

## **SURVEY CONDUCTED**

In my work capacity, I have conducted a WLAN survey from 21<sup>st</sup> – 31<sup>st</sup> January 2003 in order to gain a better understanding of the use and deployment of WLAN in organisations. The questionnaire and results of the survey are in *Annex D*.

A total of 46 organisations responded. Overall, 33 of the respondents have implemented WLAN; 8 do not have plans to implement WLAN; the remaining 5 are either in WLAN pilot trials or planning to implement WLAN in Year 2003.

The findings from the survey revealed that most organizations do not have a security policy in place to govern the implementation and use of WLAN. It was also clear that organizations had compromised on security while pursuing operational efficiency and economies of scale. While I couldn't more than agree that the security guidelines that were recommended earlier in this paper are crucial to an organization, there is also an inevitable need to strike a balance between security and operations (costs). Organisations have to understand their own needs and eventually lay down their own policies with sufficient mitigating measures to compensate on what have been compromised on.

## CONCLUSION

Organisations need to assess the security threats associated with WLAN and their security needs with respect to the confidentiality, integrity and availability of their information assets. They should also determine the appropriate level and type of security measures to be implemented to mitigate the security risks to the level that is acceptable by the organisation.

In view of the major WEP vulnerabilities and security threats posed by WLAN, confidential or important information should not be transmitted unprotected over the WLAN. Where there is a need to transmit such information via the WLAN, additional control measures such as end-to-end encryption should be used to ensure the confidentiality and integrity of the information.

It will also be prudent to treat the WLAN as a less trusted network compared to the internal wired network. Proper network segregation and access controls can be implemented to protect the organisation's internal network from the WLAN.

As attacks can be targeted on the wireless station via the WLAN, the client computing devices should not be used to store or process confidential or important information unless proper authentication and access control mechanisms have been implemented to ensure the client's security.

## REFERENCES

[1] J. R. Walker, "Unsafe at any key size; An analysis of the WEP encapsulation", IEEE 802.11-00/362, October 2000.

<http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip>

[2] W. A. Arbaugh, N. Shankar and Y. C. J. Wan, "Your 802.11 Wireless Network has No Clothes", University of Maryland, Department of Computer Science, March 2001. <http://www.securityfocus.com/data/library/wireless.pdf>

[3] Tom Karygiannis and Les Owens, "Wireless Network Security: 802.11, Bluetooth, and Handheld Devices", NIST Special Publication SP 800-48, November 2002.  
[http://csrc.nist.gov/publications/nistpubs/800-48/NIST\\_SP\\_800-48.pdf](http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf)

[4] Bob Fleck and Jordan Dimov, Cigital Inc, "Wireless Access Points and ARP Poisoning: Wireless vulnerabilities that expose the wired network".  
<http://www.cigitalabs.com/resources/papers/download/arppoison.pdf>

[5] Mishra, A & Arbaugh, W, "An initial security analysis of the 802.1x standard", Feb 2002. <http://www.cs.umd.edu/~waa/1x.pdf>

[6] Scott Fluhrer, Itsik Mantin and Adi Shamir, "Weakness in the Key Scheduling Algorithm of RC4".  
[http://www.drizzle.com/~aboba/IEEE/rc4\\_ksaproc.pdf](http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf)

[7] J. Philip Craiger, "802.11, 802.1X and Wireless Security", June 2002.  
<http://www.sans.org/rr/wireless/80211.php>

[8] Christopher W. Klaus, "Wireless LAN Security FAQ", Internet Security Systems (ISS), October 2002. [http://www.iss.net/wireless/WLAN\\_FAQ.php](http://www.iss.net/wireless/WLAN_FAQ.php)

[9] "CISCO Aironet Wireless LAN Security Overview", August 2002.  
[http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w\\_ov.htm](http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm)

[10] Robert Braid and Mike Lynn, "Advanced 802.11b Attack", July 2002.  
<http://www.blackhat.com/html/bh-usa-02/bh-usa-02-speakers.html#Baird>

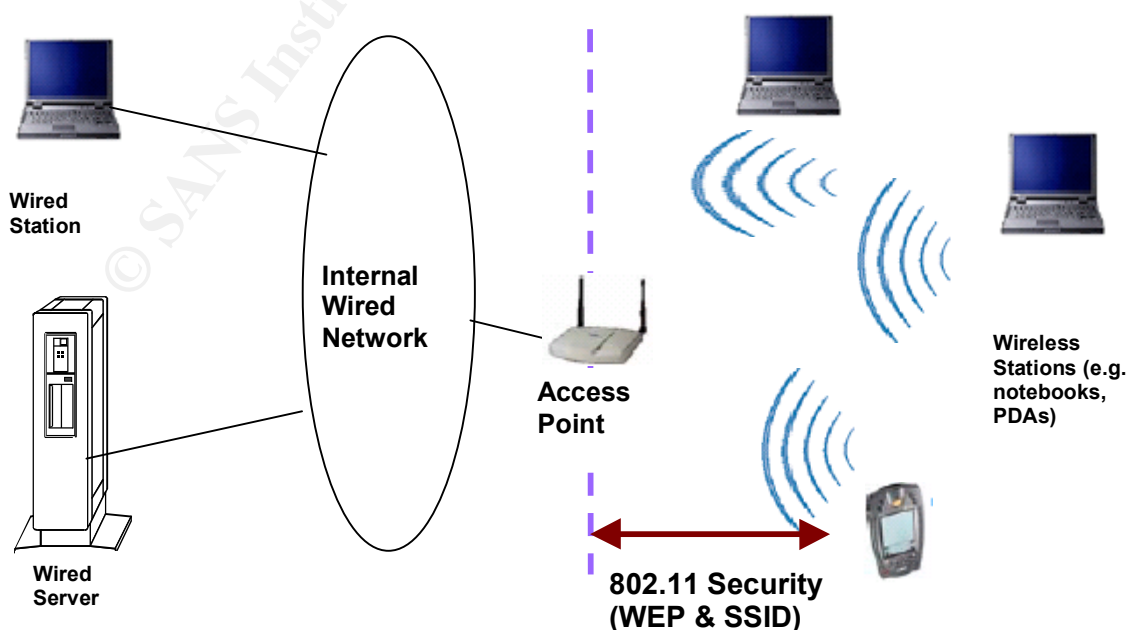
[11] Mike D. Schiffman, "The Need for 802.11b Toolkit", July 2002.  
<http://www.blackhat.com/html/bh-usa-02/bh-usa-02-speakers.html#MikeD.Schiffman>

## Annex A

**Typical Wireless LAN Implementation**

(Icons adapted from [3])

A WLAN can be configured in 2 modes, namely the **ad-hoc** or the **infrastructure** network mode. An **ad-hoc** WLAN (see Figure 1) allows wireless stations to connect directly to one another for sharing of files or resources. In an **infrastructure** WLAN (see Figure 2), wireless stations communicate with one another via the access point, which also serves as the bridge that interconnects the WLAN and the wired network. Wired Equivalent privacy (WEP) and Service Set Identifier (SSID) are the two security mechanisms in IEEE 802.11b for providing confidentiality and access control.

**Figure 1 - 802.11 WLAN Implementation In Ad Hoc Topology****Figure 2 - 802.11 WLAN Implementation In Infrastructure Topology**

## Annex B

## Summary of 802.11 Standards [3]

The following table provides a summary of the various 802.11 standards. For each of the eight standards, a description of the standard, purpose keywords and remarks about the standard, and when the standard and products will be available are provided.

Standard	Description	Purpose Keywords and Other Remarks	Availability
<b>802.11a</b>	A physical layer standard in the 5 GHz radio band. It specifies eight available radio channels (in some countries, 12 channels are permitted). The maximum link rate is <b>54 Mbps</b> 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 radio access point increases.	<b>Higher Performance.</b>  In most office environments, the data throughput will be greater than for 11b. Also, the greater number of radio channels (eight as opposed to three) provides better protection against possible interference from neighboring access points. Conformance is shown by a Wi-Fi5 mark from WiFi Alliance.	Standard was completed in 1999.  Products are available now.
<b>802.11b</b>	This is a physical layer standard in the 2.4 GHz radio band. It specifies three available radio channels. Maximum link rate is <b>11 Mbps</b> 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 radio access point increases.	<b>Performance.</b>  Products are in volume production with a wide selection at competitive prices. Installations may suffer from speed restrictions in the future as the number of active users increase, and the limit of three radio channels may cause interference from neighboring access points.	Standard was completed in 1999.  A wide variety of products have been available since 2001.
<b>802.11d</b>	This standard is supplementary to the Media Access Control (MAC) layer in 802.11 to promote worldwide use of 802.11 WLANs. It will allow access points to communicate information on the permissible radio channels with acceptable power levels for user devices. The 802.11 standards cannot legally operate in some countries; the purpose of 11d is to add features and restrictions to allow WLANs to operate within the rules of these	<b>Promote worldwide use.</b>  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.	Work is ongoing, but see 802.11h for a timeline on 5 GHz WLANs in Europe.

	countries.		
<b>802.11e</b>	This standard is supplementary to the MAC layer to provide QOS support for LAN applications. It will apply to 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.	<p><b>Quality of service.</b></p> <p>This standard should provide some useful features for differentiating data traffic streams. It is essential for future audio and video distribution. Many WLAN manufacturers have targeted QOS as a feature to differentiate their products, so there will be plenty of proprietary offerings before 11e is complete. This standard will be greatly affected by the work of TGi.</p>	The standard is still in draft version 5.0.
<b>802.11f</b>	This is a "recommended practice" document that aims to achieve radio access point interoperability within a multi-vendor WLAN network. The standard defines the registration of access points within a network and the interchange of information between access points when a user is handed over from one access point to another.	<p><b>Interoperability.</b></p> <p>This standard will work to increase vendor interoperability. Currently few features exist in the AP work. 802.11f will reduce vendor lock-in and allow multi-vendor infrastructures.</p>	<p>Completed standard in second half of 2002.</p> <p>Products available.</p>
<b>802.11g</b>	This is a physical layer standard for WLANs in the 2.4 GHz and 5 GHz radio band. It specifies three available radio channels. The maximum link rate is <b>54 Mbps</b> per channel whereas 11b has 11 Mbps. The 802.11g standard uses orthogonal frequency-division multiplexing (OFDM) modulation but, for backward compatibility with 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.	<p><b>Performance with 802.11b backward compatibility.</b></p> <p>Speeds similar to 11a and backward compatibility may appear attractive but modulation issues exist: Conflicting interests between key vendors have divided support within IEEE task group for the OFDM and PBCC modulation schemes. The task group compromised by including both types of modulation in the draft standard. With the addition of support for 11b's CCK modulation, the end result is three modulation types. This is perhaps too little, too late, and too complex relative to 11a. However, advantages exist for vendors hoping to supply dual-mode 2.4 GHz and 5 GHz products, in that using OFDM for both modes will reduce silicon cost. If</p>	<p>Completed standard in first half of 2003.</p> <p>Products available.</p>

		802.11h fails to obtain pan-European approval by the second half of 2003, then 11g will become the high-speed WLAN of choice in Europe.	
<b>802.11h</b>	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.	<p><b>European regulation compliance.</b></p> <p>This is necessary for products to operate in Europe. Completion of 11h will provide 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 ETSI. Although European countries such as the Netherlands and the United Kingdom are likely to allow the use of 5 GHz LANs with TPC and DFS well before 11h is completed, pan-European approval of 11h is not expected until the second half of 2003 or later.</p>	<p>Completed standard in third half of 2002.</p> <p>No further information on products availability.</p>
<b>802.11i</b>	This standard is supplementary to the MAC layer to improve security. It will apply to 802.11 physical standards a, b, and g. It provides an alternative to Wired Equivalent Privacy (WEP) with new encryption methods and authentication procedures. IEEE 802.1X forms a key part of 802.11i.	<p><b>Improved security.</b></p> <p>Security is a major weakness of WLANs. Vendors have not improved matters by shipping products without setting default security features. In addition, the numerous Wired Equivalent Privacy (WEP) weaknesses have been exposed. The 802.11i specification is part of a set of security features that should address and overcome these issues by the end of 2003. Solutions will start with firmware upgrades using the Temporal Key Integrity Protocol (TKIP), followed by new silicon with AES (an iterated block cipher) and TKIP backwards compatibility.</p>	Standard is still in draft version 5.0.



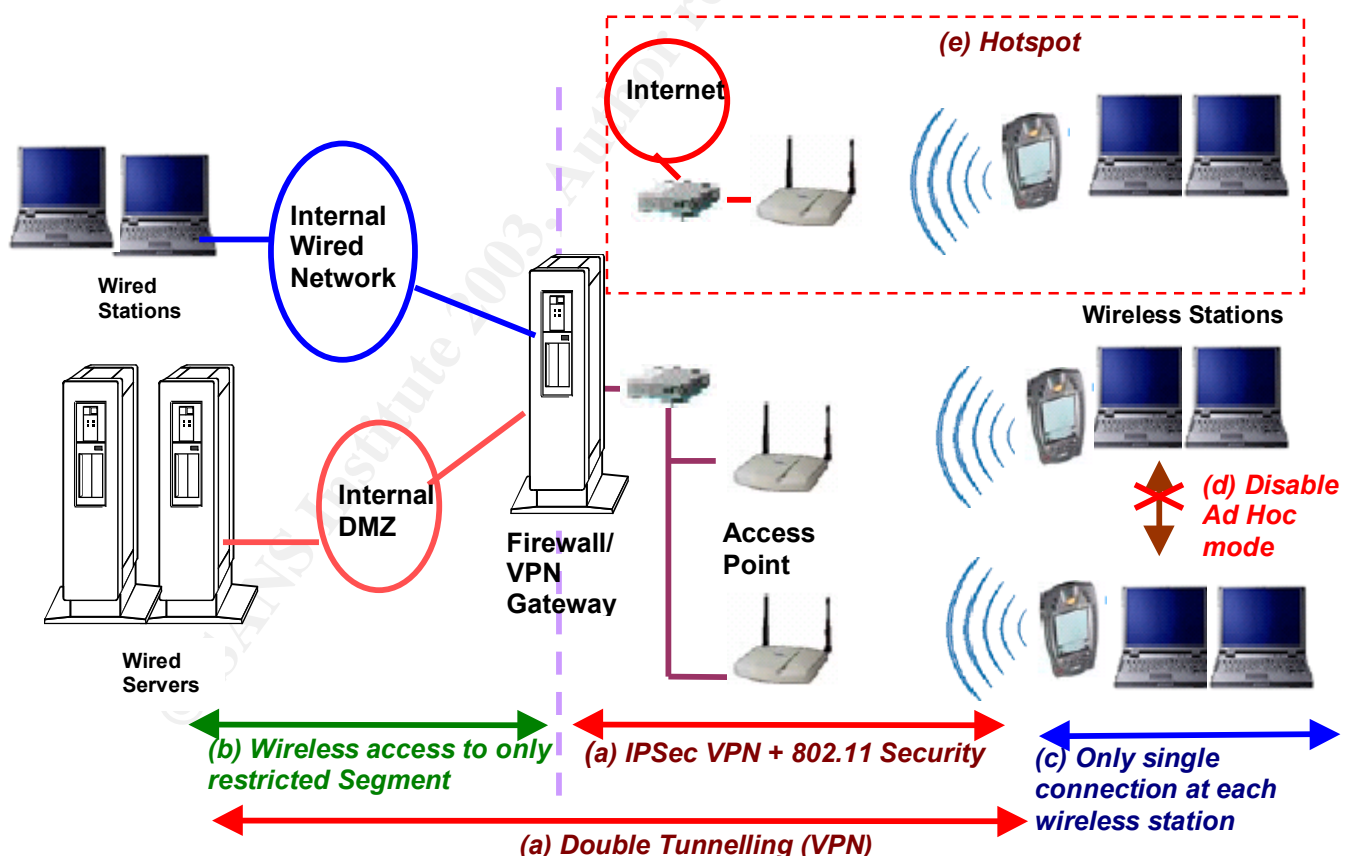
## Annex C

**Proposed WLAN Implementation In Office Environment**

(Icons adapted from [3])

Figure 3 illustrates the proposed WLAN implementation:

- Implement IPSec-based VPN or equivalent technology (on top of 802.11 security mechanism) to protect the wireless communication. Consider "Double tunnelling" to provide end-to-end confidentiality protection if necessary. This is to establish a secure tunnel between two end points. To ensure authenticity and confidentiality of the wireless communication without solely relied on 802.11 security mechanisms.
- Implement access control mechanism (e.g. firewall) to segregate and restrict all wireless access within a segment (e.g. DMZ) of the corporate LAN. This is to prevent any wireless activities from compromising the security of the wired network and disrupt operations.
- Only allows single connection at each wireless station at any one time. This is to prevent the use of the wireless station as a bridging device between two networks.
- Disable ad hoc mode between wireless stations.
- WLANs that are deployed as Hotspots for public's access to Internet shall be physically separated from the internal network.

**Figure 3 - Proposed WLAN Implementation In Office Environment**

## Proposed WLAN Implementation In Home Environment

(Icons adapted from [3])

Figure 4. illustrates the proposed WLAN implementation:

- Implement IPSec based VPN or equivalent technology to secure wireless communication.
- Implement appropriate security control to protect wireless station. These include client hardening, disable unnecessary services and files sharing, install anti-virus software and personal firewall etc.
- Disable ad hoc mode.

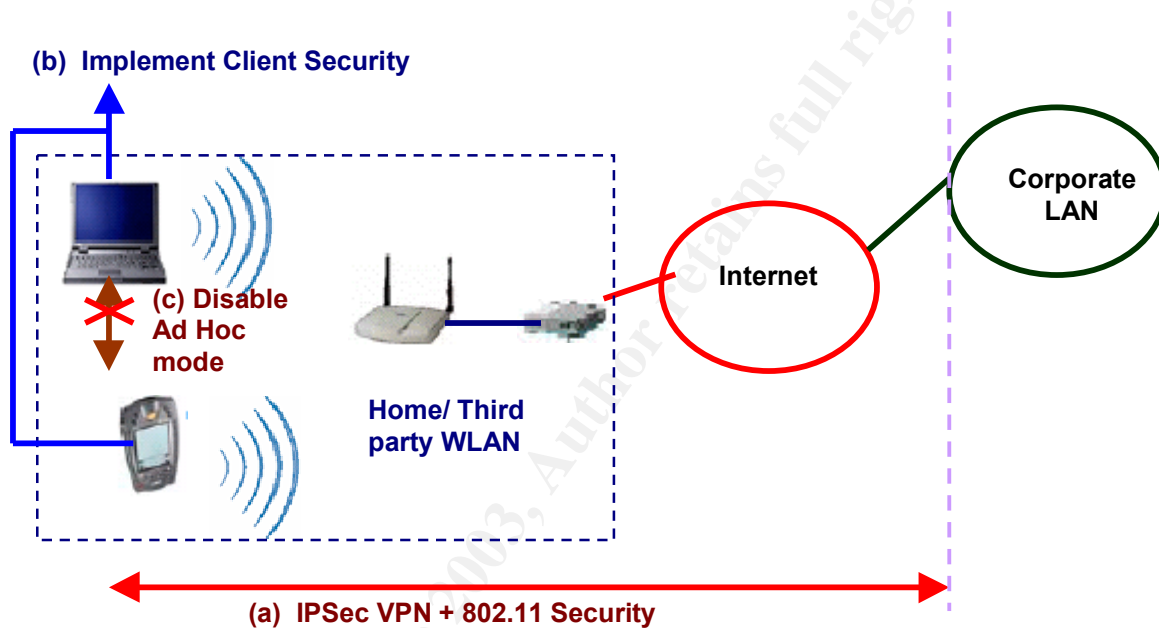


Figure 4 - Proposed WLAN Implementation In Home Environment

## Annex D

## WLAN Survey Questionnaires &amp; Results

A total of 46 agencies responded out of 80 agencies surveyed. Certain questions have been sanitized as they contain sensitive information.

1. Is your organisation currently using or planning to deploy WLAN?

	Results	
	Total	Percentage
Implemented	33	72%
Have plans to implement (including trial/pilot)	5	11%
No Plans	8	17%

2. Is there a security policy in your organisation that addresses the use and security aspects of wireless technology, including WLAN?

	Results	
	Total	Percentage
Yes	15	45%
No	18	55%

3. Is your organisation aware of the Wireless LAN Security Best Practices that is published in our website? Have your organisation adopted the security best practices in your deployment? If YES, what are some areas of improvement to make it more useful to your organisation? If NO, Why?

Summary Of Remarks	
1	Yes. Guidelines for a. Conducting risk assessment b. Conducting spillage of WLAN c. Methods to prevent user from installing or running network sniffer
2	Yes. A Special Interest Group (SIG) on WLAN security
3	Yes. Project halted and will be seeking additional funding to purchase the necessary solution to meet the WLAN security guidelines.
4	Yes. Provide examples of VPN or other security products that have been approved for use over WLAN.
5	Yes. Adoption of 802.1 standard to improve security.
6	Yes. It is not practical nor cost effective to deploy WLAN if a full firewall and VPN solution is required – the latter is more appropriate with enterprise WLAN access protection
7	No. Not aware of the availability of the best practices until now.
8	To have a checklist and recommended tools to detect rouge APs
9	More information on the development of 802.11a security features will be helpful
10	Yes. Including links to best of breed WLAN security technology in the document
11	Yes. Provide more update information (on the Intranet) about the latest security vulnerabilities and trends pertaining to WLAN. The WLAN security best practices should also be regularly revised.

4. What is the primary use of WLAN in your organisation for? Please further elaborate the use of WLAN by using "Further Details" box below.

	Results	
	Total	Percentage
Provide wireless access to Internet ONLY	2	6%
Provide wireless access to corporate resources and information that are <u>unclassified</u>	8	24%
Provide wireless access to corporate resources and information that are <u>classified up to confidential</u>	20	61%
Provide wireless access to corporate resources and information that are <u>classified above confidential</u>	0	0%
Others	3	9%

5. What do you think are the major security concerns in implementing WLAN in a large multinational organisation? Please check TOP THREE concerns that apply:

	Results
	Total
How to secure WLAN implementation (i.e. Design & configure).	22
Weak authentication implementation provided by IEEE802.11 WLAN standards.	20
Weak cryptographic implementation (i.e. WEP) provided by IEEE 802.11 WLAN standards.	18
No effective solution in detecting unauthorized equipments (i.e. client devices and access points) deploy by malicious entities.	15
Degradation in network and/or system performance with VPN over WLAN.	12
No effective solution in preventing Denial-of-Service (DoS) within WLAN.	7
APs and WLAN being listed or published by entities conducting War Driving.	5
Others. Please specify:	0

6. What are some of the security measures that your organisation had implemented or would consider to implement for WLAN within the next 6 months? Please check all that apply:

	Results
	Total
<b><u>a. Physical Security</u></b>	
Keep an inventory of all APs and 802.11 wireless devices including procedure in wireless devices handling, use and disposal and lost/theft incidents.	19
Locate APs within physically protected office environment.	18
Locate APs in secured areas (i.e. Box with lock) to prevent unauthorised physical access and user manipulation.	9
Conduct site survey to measure and establish AP coverage within building perimeters. (Periodic checks for sensitive areas)	13
<b><u>b. APs Management</u></b>	
Ensure that all default parameters (i.e. SSID, password, channel, cryptographic key etc) are changed.	21
Implement MAC access control list for both APs and wireless devices.	16
Turn off APs when not in use (i.e. off-office hour).	5
Implement mutual authentication for both wireless devices & APs.	13

Ensure dedicated and secure APs management (i.e. SNMPv3, SSL/TLS) via wired link. (Existing APs do not support SSL/TLS or SNMPv3)	7
<b><u>c. User Authentication</u></b>	
Implement strong user authentication (i.e. Two-factor authentication).	10
<b><u>d. Confidentiality &amp; Integrity</u></b>	
Implement dynamic WEP key with minimum 128bit in key sizes.	16
Implement VPN over WLAN.	10
<b><u>e. Access Controls</u></b>	
Segregate WLAN from wired network with access control filtering device (i.e. Firewall, router).	15
Allow wireless access to only restricted segment of wired network (i.e. DMZ).	4
Implement IEEE 802.1x port-based network access control.	9
Disable DHCP and use static IP addresses.	5
Disable file and print share.	1
<b><u>f. Intrusion Detection &amp; Monitoring</u></b>	
Implement wireless IDS to detect suspicious behaviour or unauthorised access and activity (i.e. peer-to-peer wireless clients, rogue access points and wireless client etc).	3
<b><u>g. Client Security</u></b>	
Implement client protection with anti-virus and personal firewall solution	18
Disable sharing of file.	5
<b><u>h. Logging &amp; Audit Trail</u></b>	
Implement logging and auditing technology to analyse APs and server logs for suspicious activity.	19
<b><u>i. Awareness &amp; Training</u></b>	
Ensure that users are trained in computer security awareness and the risks associated with WLAN.	20