Australian Government
Department of Defence
Intelligence and Security

PROTECT

Security for Wireless Networks

Defence Signals Directorate - Cyber Security Operations Centre

January 2012

Contents

Introduction

1. Wireless networks are increasingly being used by organisations. This is due to their ease of deployment, low cost compared to traditional fixed networks and to satisfy employee demand. This document provides technical guidance on the use of wireless networks.

Intended Audience

2. This document is intended for information security professionals within organisations.

Security Considerations

3. The confidentiality, integrity and availability risks associated with the use of wireless networks, as well as recommendations to assist in reducing these risks, are discussed in detail below. An overview of recommendations is available at Attachment B.

Wireless networks for public use

4. When an organisation introduces wireless networks for public access e.g. a public hotspot, such wireless networks should not be connected to any networks that communicate or store sensitive information. Allowing a connection between such networks could provide an easily accessible entry point for an adversary to target a connected fixed network to steal sensitive information or disrupt services.

Connecting wireless networks to fixed networks

5. When an organisation has a business requirement to connect a wireless network to a fixed network, it is important that they consider the security risks. While fixed networks are often afforded a certain degree of physical security, wireless networks due to their nature are often easily accessible outside of the controlled perimeter of an organisation. To protect against an attack originating from a wireless network against a fixed network, connections between wireless networks and fixed networks should be treated in the same way organisations would treat connections between fixed networks and the Internet. For example, by implementing a gateway to inspect and control the flow of information between the two networks.

Compatibility of wireless access points

6. Wireless access points that have been certified against a Wi-Fi Alliance certification program[1] should be used for wireless networks as they provide an organisation with the assurance that they conform to wireless standards. Deploying wireless access points that are guaranteed to be interoperable with other wireless access points on a wireless network will prevent any problems on the network due to incompatibility of wireless standards supported or incorrect implementation of wireless standards by vendors.

[1] http://wi-fi.org/certification_programs.php

Default user names and passwords for wireless access points

7. Wireless access points come pre-configured with default accounts and passwords that are freely available in product documentation and online forums. For example, it is common for wireless access points to come pre-configured with an administrator account named “admin” and a password of either “admin” or “password”. To ensure default user names and passwords aren’t exploited to gain unauthorised access to wireless access points, default user names and passwords should be changed before wireless access points are deployed in a wireless network.

Unused physical network ports on wireless access points

8. If unused physical network ports are left enabled on wireless access points they could allow an adversary to directly connect to a connected fixed network, connect to an administrative interface via a wired connection or connect another compromised wireless access point to the network. To prevent this from occurring, any unused physical network ports on wireless access points should be disabled.

Administrative interfaces for wireless access points

9. Administrative interfaces allow users to modify the configuration and security settings of wireless access points. Often wireless access points by default allow users to access the administrative interface over methods such as fixed network connections, wireless network connections and serial connections directly on the device. To prevent an adversary connecting to wireless access points, the administrative interface on wireless access points should be disabled for wireless connections.

Default service set identifiers

10. All wireless access points come with a default Service Set Identifier (SSID). The SSID is commonly used to identify the name of a wireless network to users. As the default SSIDs of wireless access points are well documented on online forums, along with default accounts and passwords, the default SSID of wireless access points should be changed.

11. When changing the default SSID, it is important that it lowers the profile of an organisation’s wireless network to adversaries. In doing so, the SSID of a wireless network should not be readily associated with an organisation, the location of or within their premises, or the functionality of the network.

12. A method commonly recommended to lower the profile of wireless networks is disabling SSID broadcasting. While this ensures that the existence of wireless networks are not broadcast overtly using beacon frames, the SSID is still broadcast in probe requests, probe responses, association requests and re-association requests for the network. Knowledgeable adversaries will still be able to determine the SSID of wireless networks by capturing these requests and responses. By disabling SSID broadcasting organisations will make it more difficult for users to connect to wireless networks as legacy operating systems only have limited support for hidden SSIDs. In addition, a security risk exists where an adversary can configure a wireless access point to broadcast the same SSID as the hidden SSID used by a legitimate wireless network. In this scenario devices will automatically connect to the wireless access point that is broadcasting the SSID they are configured to use before probing for a wireless access point that accepts the hidden SSID. Once the device is

connected to the adversary's wireless access point the adversary can steal authentication credentials from the device to perform a man-in-the-middle attack to capture legitimate wireless network traffic or to later reuse to gain access to the legitimate wireless network. For these reasons SSID broadcasting should be enabled on wireless networks.

Static addressing

13. Assigning static IP addresses for devices accessing wireless networks can prevent a rogue device when connecting to a network from being assigned a routable IP address. However, knowledgeable adversaries will be able to determine IP addresses of legitimate users and use this information to guess or spoof valid IP addresses ranges for wireless networks. As configuring devices to use static IP addresses introduces a management overhead without any tangible security benefit, the dynamic host configuration protocol should be used for assigning IP addresses on wireless networks.

Media Access Control address filtering

14. Devices that connect to wireless networks have a unique Media Access Control (MAC) address. It is possible to use MAC address filtering on wireless access points to restrict which devices can connect to wireless networks. While this approach will introduce a management overhead of configuring whitelists of approved MAC addresses, it can prevent rogue devices from connecting to wireless networks. However, knowledgeable adversaries will be able to determine valid MAC addresses of legitimate users already on wireless networks and use this information to spoof valid MAC addresses and gain access to a network. As MAC address filtering introduces a management overhead without any tangible security benefit, MAC address filtering should not be used on wireless networks.

Authentication of wireless access points and devices

15. When deploying a wireless network, an organisation will need to determine whether they will deploy the network with robust security to protect sensitive information or with no security for their clients or the public to access e.g. a public hotspot.

16. If deploying a public hotspot, an organisation may opt for no authentication for devices. Deploying a wireless network with no authentication allows any device to connect to the network without having to pre-configure the device with network settings. While this provides ease of use for the public, it also provides a number of security risks to an organisation, such as criminal misuse.

17. Where an organisation chooses to secure a wireless network, they can choose from a number of Extensible Authentication Protocol (EAP) methods that are supported by the Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) security protocols. As WPA2 has superseded WPA, for the remainder of this document WPA2 variants will be referred to.

18. Organisations deploying a secure wireless network should choose WPA2-Personal with Pre-Shared Key (PSK), WPA2-Enterprise with EAP-Transport Layer Security (EAP-TLS), WPA2-Enterprise with EAP-Tunnelled Transport Layer Security (EAP-TTLS) or WPA2-Enterprise with Protected EAP (PEAP) to perform mutual authentication. An organisation's choice in authentication method will often be based on the size of their deployment, their security requirements and any existing authentication infrastructure they plan on utilising.

19. Each of the EAP methods discussed below has its own advantages and disadvantages and will be discussed briefly. If an organisation is primarily motivated by security they can implement either PEAP-EAP-TLS or EAP-TLS. If they are primarily motivated by flexibility and legacy support they can implement EAP-TTLS. If they are primarily motivated by simplicity they can implement PEAP with EAP-MSCHAPv2.

Extensible Authentication Protocol methods for authentication

20. IEEE 802.1X is an authentication mechanism supported by WPA2-Enterprise for encapsulating EAP methods over wireless networks. EAP in turn is an authentication framework used by wireless networks that allows for the generation and communication of keying material used by EAP methods that perform authentication services. A number of EAP methods such as EAP-TLS, EAP-TTLS and PEAP perform mutual authentication. Mutual authentication ensures that devices can be authenticated by wireless access points and that devices can authenticate wireless access points.

21. The initial release of the WPA2 security protocol supported two modes, WPA2-Personal and WPA2-Enterprise. WPA2-Personal was aimed at small wireless deployments within the home, small business or low support environments and used a PSK for authentication. WPA2-Enterprise was aimed at large wireless deployments within the corporate environment and used either the password-based Lightweight EAP (LEAP) or certificate-based EAP-TLS method.

22. To address the lack of support for alternative EAP methods in WPA2-Enterprise, the WPA2 standard was updated. Two additional EAP methods of interest were EAP-TTLS and PEAP. Both of these EAP methods eliminated the need for device-side certificates required by EAP-TLS yet still leveraged a server-side certificate to create a secure TLS tunnel from within which EAP authentication could take place.

Authentication using WPA2-Personal with pre-shared key

23. WPA2-Personal with PSK offers an organisation the ability to authenticate devices without the use of a public key infrastructure or Remote Access Dial In User Service (RADIUS) authentication server. In WPA2-Personal with PSK, devices only authenticate to wireless access points by having knowledge of the PSK. The wireless access points do not authenticate to the devices.

24. The downside of using WPA2-Personal with PSK is that it relies on the strength of the passphrase used for a PSK to secure access to a wireless network. A knowledgeable adversary using either a brute-force attack, or rainbow tables of the most common SSIDs, may have success based on the strength of the passphrase and the SSID used when attempting to determine the PSK. Once a PSK is compromised an adversary can use it to connect to a wireless network. To reduce this security risk, a passphrase that is at least 20 characters long and consisting of random characters derived from a character set that includes upper and lower case alphabet characters, numeric characters and special characters should be used.

25. Given the right resources and time, no PSK is immune to a brute-force attack. Therefore, a PSK's passphrase should be changed on a regular basis, noting that it will have a business impact as all wireless access points and devices using a wireless network will need to be updated. If a compromise of a wireless network occurs, or a user leaves an organisation, the only recourse is to change the passphrase. If an organisation fails to change the passphrase, an ex-employee of an organisation may retain their access until such a time that it is changed. Furthermore, as PSKs are

saved on devices, any stolen device that has been configured to access an organisation's wireless network will maintain its access until the passphrase is changed.

Authentication using WPA2-Enterprise with EAP-TLS

26. WPA2-Enterprise with EAP-TLS is considered one of the most secure EAP methods. Due to its inclusion in the initial release of the WPA2 standard, it enjoys wide support in wireless access points and in numerous operating systems such as Microsoft Windows, Linux and Apple Mac OS X. EAP-TLS uses a public key infrastructure to secure communications between devices and a RADIUS authentication server through the use of X.509 certificates. While EAP-TLS provides strong mutual authentication, it requires an organisation to have established a public key infrastructure. This involves either deploying their own certificate authority and issuing certificates, or purchasing certificates from a commercial certificate authority, for every device that accesses the wireless network. While this introduces additional costs and management overheads to an organisation, the security advantages are significant.

Authentication using WPA2-Enterprise with EAP-TTLS

27. The EAP-TTLS/MSCHAPv2, or simply EAP-TTLS, method used with WPA2-Enterprise is generally supported through the use of third party software. It has support in multiple operating systems but does not have native support in Microsoft Windows. EAP-TTLS is different to EAP-TLS in that devices do not authenticate to the server when the initial TLS tunnel is created. Only the server authenticates to devices. Once the TLS tunnel has been created, mutual authentication occurs through the use of another EAP method. An advantage of EAP-TTLS over PEAP is that a username is never transmitted in the clear outside of the TLS tunnel. Another advantage of EAP-TTLS is that it provides support for many legacy EAP methods, while PEAP is generally limited to the use of EAP-MSCHAPv2.

Authentication using WPA2-Enterprise with PEAP

28. PEAPv0/EAP-MSCHAPv2, or simply PEAP, is the second most widely supported EAP method after EAP-TLS. It enjoys wide support in wireless access points and in numerous operating systems such as Microsoft Windows, Linux and Apple Mac OS X. PEAP operates in a very similar way to EAP-TTLS by creating a TLS tunnel which is used to protect another EAP method. PEAP differs from EAP-TTLS in that when the EAP-MSCHAPv2 method is used within the TLS tunnel, only the password portion is protected and not the username. This may allow an adversary to capture the username and replay it with a bogus password in order to lockout the user's account causing a denial of service for that user. While EAP-MSCHAPv2 within PEAP is the most common implementation, Microsoft Windows supports the use of EAP-TLS within PEAP, known as PEAP-EAP-TLS. This approach is very similar in operation to traditional EAP-TLS yet provides increased protection, as parts of the certificate that aren't encrypted with EAP-TLS are encrypted with PEAP-EAP-TLS. The downside to PEAP-EAP-TLS is its support is limited to Microsoft products.

Issuing certificates for authentication

29. When certificates are issued to devices that access a wireless network, an organisation needs to be aware of the security risk that these certificates could be stolen from a device through the use of malicious software. Once compromised, the certificate could be used by an adversary on

another device to gain access to the wireless network. Organisations need to be aware that in issuing a certificate to a device, any actions taken by a user will only be attributable to a device and not a specific user.

30. An alternative to issuing certificates to devices is to issue certificates to users. This can either be in the form of a certificate that is stored on a device or a certificate that is stored within a smart card. Issuing certificates on smart cards provides increased security however at a higher cost. As a user is more likely to notice a stolen smart card, they can immediately report the incident to their local security team who can revoke the credentials on the RADIUS server, hence minimising the time an adversary can gain access to a wireless network. In addition, to reduce the likelihood of a stolen smart card from being used by an adversary to gain access to a wireless network, two-factor authentication can be implemented through the use of access Personal Identification Numbers (PINs) on smart cards. This is particularly important when a smart card grants a user any form of administrative access on a wireless network or attached network resource.

31. To reduce the impact of certificates being lost or stolen, unique certificates should be issued for both devices and users. The certificates for a device and user should not be stored on the same device as theft, or compromise, of the device by an adversary would result in the compromise of both certificates. For increased security, certificates for users should be issued on smart cards with access PINs and not stored with a device when not in use.

Using commercial certification authorities for certificate generation

32. A security risk exists with EAP-TTLS and PEAP when a commercial certificate authority's certificates are automatically trusted by devices using vendor trusted certificate stores. This trust can be exploited by an adversary who obtains certificates from a commercial certificate authority under false pretences as they can trick devices into trusting their signed certificate. This will allow the adversary to capture authentication credentials presented by devices, which in the case of EAP-MSCHAPv2, can be cracked using a brute-force attack granting not only network access but most likely Active Directory credentials as well. To reduce this security risk, devices should be configured to validate the server certificate, disable any trust for certificates generated by commercial certificate authorities that aren't trusted and disable the ability to prompt users to authorise net servers or commercial certificate authorities. Additionally, devices should be set to enable identity privacy which will prevent their username being sent prior to being authenticated by the RADIUS server.

Caching authentication outcomes

33. When IEEE 802.1X authentication is used, a shared secret key known as the Pairwise Master Key (PMK) is generated. Upon successful authentication of a device, the PMK is capable of being cached to assist with fast roaming between wireless access points. When a device roams away from a wireless access point that it has authenticated to, it will not need to perform a full re-authentication should it roam back while the cached PMK remains valid. To further assist with roaming, wireless access points can be configured to pre-authenticate a device to other neighbouring wireless access points that the device might roam to. Although requiring full authentication for a device each time it roams between wireless access points is ideal, organisations can chose to use PMK caching and pre-authentication if they have a business requirement for fast

roaming. If PMK caching is used, the PMK caching period should not be set to greater than 1440 minutes (24 hours).

Encryption of wireless traffic

34. As wireless transmissions are capable of radiating outside of secured areas, organisations can't rely on the traditional approach of physical security to protect against an adversary capturing information on wireless networks. As such, wireless networks need to be encrypted to maintain the confidentiality of information that is being passed over the networks. Organisations should use the Advanced Encryption Standard (AES) based Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) to protect the confidentiality of all wireless network traffic. Organisations looking for additional security through a layered approach to encryption, can implement a virtual private network over the top of CCMP.

35. CCMP was introduced in WPA2 to address feasible attacks against the Temporal Integrity Key Protocol (TKIP) used by WPA as well as the original Wireless Encryption Protocol (WEP). An adversary looking to exploit vulnerabilities in TKIP and WEP can attempt to connect to wireless access points using one of these protocols. By default, wireless access points will attempt to accommodate this request by falling back to a legacy protocol that the device supports. To ensure that wireless access points do not fall back to an insecure encryption protocol, TKIP and WEP support should be disabled or removed from wireless access points.

36. For optimal cryptographic security, both WPA2-Enterprise and WPA2-Personal in Microsoft Windows offer the ability to enforce US Government's Federal Information Processing Standards (FIPS) compliance for wireless networks. This ensures that implementations of cryptographic algorithms that have not been FIPS validated will not be used.

Interference between wireless networks

37. Where multiple wireless networks are deployed in close proximity, there is the potential for interference to impact on the availability of the network, especially when networks are operating on commonly used default channels of 1 and 11. To reduce this risk, wireless networks should be sufficiently separated through the use of channel separation. This can be achieved by using wireless networks that are configured to operate on channels that are at least one apart. For example, channels 1, 3 and 5 could be used to separate three wireless networks.

Wireless intrusion detection and prevention

38. Special anomaly detection techniques can be used by wireless intrusion detection systems and wireless intrusion prevention systems. Wireless intrusion detection systems will raise alerts to system administrators when any anomalous activity is detected on wireless networks; while wireless intrusion prevention systems are capable of automatically quarantining suspected rogue devices from wireless networks until they can be assessed by system administrators. Either a wireless intrusion detection system or wireless intrusion prevention system should be used on wireless networks.

Time synchronisation between network devices

39. When attacks occur against wireless networks, or via a wireless network against a connected fixed network, it is critical that any events logged from wireless access points can be correlated with other network devices and their event logs. To ensure this occurs, all clocks should be synchronised between wireless access points and other network devices. This is generally achieved through the use of a dedicated time server on the network.

Use of Simple Network Management Protocol

40. The Simple Network Management Protocol (SNMP) can be used to monitor the status of wireless access points. The first two iterations of SNMP were inherently insecure as they used trivial authentication methods. If an organisation requires the use of SNMP, SNMPv3 should be used, otherwise SNMP should be disabled. Furthermore, all default SNMP community strings should be changed on wireless access points and access should be limited to read only access.

Use of Wi-Fi Protected Setup

41. Wi-Fi Protected Setup (WPS) provides a convenient way for organisations to connect wireless access points and devices to wireless networks using that use a PSK. Unfortunately, a serious flaw has been discovered in the WPS protocol. This flaw allows a wireless access point's WPS PIN to be easily brute-forced within a number of hours. Once the PIN for WPS has been determined, the PSK can immediately be retrieved granting access to the wireless network. To reduce this security risk, WPS functionality in wireless access points should be disabled. If disabling WPS is not possible, or disabling WPS in the wireless access point is found to have no effect, organisations are advised to contact their device vendor for any pending firmware upgrades or additional mitigation advice.

Protecting management frames on wireless networks

42. Effective denial-of-service attacks can be performed by exploiting unprotected management frames using inexpensive commercial hardware. The latest release of the 802.11 standard provides no protection for management frames and therefore does not prevent spoofing or denial-of-service attacks. However, 802.11w was ratified in 2009 and specifically addresses the protection of management frames on wireless networks. Where possible wireless access points and devices should be upgraded to support the 802.11w amendment.

Updating firmware for wireless access points

43. The operation of wireless access points is controlled by software known as firmware. Periodically wireless access point vendors will release updated firmware to fix software bugs, resolve security issues and add new functionality and features. A security risk exists for organisations that don't update the firmware for wireless access points as known software bugs and security issues may be exploited by an adversary to gain access to their wireless networks. To assist in reducing this security risk, firmware for wireless access points should be kept up-to-date.

Accounting for wireless access points

44. To assist in determining whether wireless access points on wireless networks are rogue, an inventory of authorised wireless access points should be maintained and audited on a regular basis.

45. Manual methods that may be used to detect wireless access points include wireless network scans and physical inspections while automated methods include network access controls and wireless intrusion detection systems and wireless intrusion prevention systems. Whichever audit method is used, it should be able to detect the presence of wireless network cards inserted into or hidden inside systems, portable devices connected to workstations via USB ports and devices attached to a network port, or other network devices such as a router or switch. It is important to note that network scans conducted over a network may not be able to detect wireless access points hidden inside workstations or connected via USB ports.

46. Auditing of wireless access points that are being added or removed from both fixed and wireless networks should be implemented. This may indicate that an adversary is attempting to introduce a backdoor into a network or attempting to conduct a denial-of-service attack against the wireless network infrastructure. As such, an organisation's incident response plan should cover appropriate actions to take place when wireless security incidents are identified.

Controlling physical access to wireless access points

47. Adequate physical protection should be provided to wireless access points, especially those in public areas, to prevent an adversary physically damaging a wireless access points in order to cause a denial of service to a wireless network.

48. Physical access to wireless access points can allow an adversary to reset devices to factory default settings by pressing a physical reset button, using a serial interface on a device or connecting directly to a device to bypass any access controls. Resetting an access point back to factory default settings may disable security settings on the device including authentication and encryption functions as well as resetting administrator accounts and passwords to known defaults. Even if access to a wireless network is not gained by resetting a wireless access point, it is highly likely a denial of service will occur.

49. Physical access to wireless access points can be restricted through methods such as physical enclosures that prevent access to console ports and factory reset buttons, mounting devices on ceilings or behind walls, or placing devices in locked rooms or cabinets.

Securing devices accessing wireless networks

50. Devices used to access wireless networks have the potential to have been exposed to viruses, malware or other malicious code. This presents a security risk as these devices could inadvertently be infecting other devices on wireless networks, leveraging a user's legitimate access to steal an organisation's sensitive information or impacting the availability of wireless networks. To assist in reducing this security risk, all reasonable measures should be taken to ensure the security of devices connecting to wireless networks.

51. Key measures that can be used to assist in securing devices that connect to wireless networks include:

- using the latest version of the operating system and applications
- applying the latest security patches to the operating system and applications
- using an anti-virus or Internet security product with up to date definition files
- using a personal firewall that provides both inbound and outbound traffic filtering
- removing all unapproved applications
- using application whitelisting to ensure only approved applications are run
- ensuring general user accounts are used instead of administrator accounts
- using strong passwords for user accounts that are changed on a regular basis; and
- disabling file sharing features.

52. Devices should be validated as secure through the use of network access control before being granting access to wireless networks. With network access control, system administrators can set policies for system health requirements. This can include a check that all operating system patches are up to date, an anti-virus program is installed and all signatures are up to date, and that a software firewall is installed and being used. Devices that comply with all health requirements can be granted access to wireless networks while devices that aren't healthy can be quarantined or granted limited access.

53. Credentials stored on devices that access wireless networks should be protected by implementing full disk encryption. This will also protect any information that a user may have downloaded to their device when accessing an organisation's wireless network and any connected fixed network. It is important to note however that the use of full disk encryption is only effective when devices have been powered off.

Bridging networks

54. Allowing devices that are connected to an organisation controlled network to simultaneously connect to another non-organisation controlled network allows the devices to act as a gateway by bridging the two networks. This opens an attack vector into an organisation controlled network. Likewise, if a user establishes a secure virtual private network session to their organisation and then connects to a public hotspot they may be opening a backdoor into their organisation's wireless network. Support for the following features on devices that connect to wireless networks should be disabled: ad hoc networks, routing between virtual private network interfaces and other network interfaces, and Internet connection sharing.

Wireless network footprint

55. Minimising the output power of wireless access points will reduce the footprint of wireless networks. Instead of deploying a small number of wireless access points that broadcast on high power, more wireless access points that use minimal broadcast power should be deployed to achieve the desired wireless network footprint. This has the added benefit of providing redundancy for a wireless network should a wireless access point become unserviceable. In such a case, the output power of other wireless access points can be increased to cover the footprint gap until the unserviceable wireless access point can be replaced.

56. An additional method to limit a wireless network's footprint is through the use of radio frequency shielding on an organisation's premises. While expensive, this will limit the wireless communications to areas under the control of an organisation. Radio frequency shielding on an organisation's premises has the added benefit of preventing an adversary from jamming wireless networks from outside of the premises in which wireless networks are operating.

Further Information

57. Further information on security measures that can be implemented to protect wireless networks can be found in the *Australian Government Information Security Manual* (ISM)[2].

Contact Details

58. Australian government agencies seeking clarification about this document can contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or assist@dsd.gov.au.

[2] http://www.dsd.gov.au/infosec/ism/

Attachment A Glossary of Abbreviations

AES	Advanced Encryption Standard
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
EAP	Extensible Authentication Protocol
EAP-TLS	EAP-Transport Layer Security
EAL-TTLS	EAP-Tunnelled Transport Layer Security
FIPS	Federal Information Processing Standards
ISM	*Australian Government Information Security Manual*
LEAP	Lightweight EAP
MAC	Media Access Control
PEAP	Protected EAP
PIN	Personal Identification Number
PMK	Pairwise Master Key
PSK	Pre-Shared Key
RADIUS	Remote Access Dial In User Service
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
TKIP	Temporal Integrity Key Protocol
WEP	Wireless Encryption Protocol
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPS	Wi-Fi Protected Setup

Attachment B Overview of Recommendations

This section provides a non-exhaustive list of wireless network security recommendations. Each recommendation listed has a reference to the associated paragraph in this document.

Wireless network security recommendations include:

- When wireless networks are deployed for the purpose of allowing uncontrolled and unknown devices to connect for Internet access e.g. a public hotspot, such wireless networks should not be connected to any networks that may communicate or store sensitive information. (4)
- Connections between wireless networks and fixed networks should be treated in the same way organisations would treat connections between fixed networks and the Internet. (5)
- Wireless access points that have been certified against a Wi-Fi Alliance certification program[3] should be used for wireless networks. (6)
- Default user names and passwords should be changed before wireless access points are deployed in a wireless network. (7)
- Any unused physical network ports on wireless access points should be disabled. (8)
- The administrative interface on wireless access points should be disabled for wireless connections. (9)
- The default SSID of wireless access points should be changed. (10)
- The SSID of a wireless network should not be readily associated with an organisation, the location of or within their premises, or the functionality of the network. (11)
- SSID broadcasting should be enabled on wireless networks. (12)
- The dynamic host configuration protocol should be used for assigning IP addresses on wireless networks. (13)
- MAC address filtering should not be used on wireless networks. (14)
- Organisations deploying a secure wireless network should choose WPA2-Personal with Pre-Shared Key (PSK), WPA2-Enterprise with EAP-Transport Layer Security (EAP-TLS), WPA2-Enterprise with EAP-Tunnelled Transport Layer Security (EAP-TTLS) or WPA2-Enterprise with Protected EAP (PEAP) to perform mutual authentication. (18)
- *If using WPA2-Personal with PSK for authentication:* A passphrase that is at least 20 characters long and consisting of random characters derived from a character set that includes upper and lower case alphabet characters, numeric characters and special characters should be used. (24)
- *If using certificate-based authentication:* Unique certificates should be issued for both devices and users. (31)
- *If using certificate-based authentication:* The certificates for a device and user should not be stored on the same device. (31)
- *If using certificate-based authentication:* Certificates for users should be issued on smart cards with access PINs and not stored with a device when not in use. (31)
- *If using certificate-based authentication:* Devices should be configured to validate the server certificate, disable any trust for certificates generated by commercial certificate authorities that aren't trusted and disable the ability to prompt users to authorise new servers or commercial certificate authorities. (32)

[3] http://wi-fi.org/certification_programs.php

- ☐ *If using certificate-based authentication:* Devices should be set to enable identity privacy. (32)
- ☐ *If using WPA2-Enterprise:* The PMK caching period should not be set to greater than 1440 minutes (24 hours). (33)
- ☐ Organisations should use the Advanced Encryption Standard (AES) based Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) to protect the confidentiality of all wireless network traffic. (34)
- ☐ TKIP and WEP support should be disabled or removed from wireless access points. (35)
- ☐ Wireless networks should be sufficiently separated through the use of channel separation. (37)
- ☐ Either a wireless intrusion detection system or wireless intrusion prevention system should be used on wireless networks. (38)
- ☐ All clocks should be synchronised between wireless access points and other network devices. (39)
- ☐ If an organisation requires the use of SNMP, SNMPv3 should be used, otherwise SNMP should be disabled. (40)
- ☐ All default SNMP community strings should be changed on wireless access points and access should be limited to read only access. (40)
- ☐ *If using WPA2-Personal:* WPS functionality in wireless access points should be disabled. (41)
- ☐ Where possible wireless access points and devices should be upgraded to support the 802.11w amendment. (42)
- ☐ Firmware for wireless access points should be kept up-to-date. (43)
- ☐ An inventory of authorised wireless access points should be maintained and audited on a regular basis. (44)
- ☐ Whichever audit method is used, it should be able to detect the presence of wireless network cards inserted into or hidden inside systems, portable devices connected to workstations via USB ports and devices attached to a network port, or other network devices such as a router or switch. (45)
- ☐ Auditing of wireless access points that are being added or removed from both fixed and wireless networks should be implemented. (46)
- ☐ An organisation's incident response plan should cover appropriate actions to take place when wireless security incidents are identified. (46)
- ☐ Adequate physical protection should be provided to wireless access points, especially those in public areas. (47)
- ☐ All reasonable measures should be taken to ensure the security of devices connecting to wireless networks. (50)
- ☐ Devices should be validated as secure through the use of network access control before being granting access to wireless networks. (52)
- ☐ Credentials stored on devices that access wireless networks should be protected by implementing full disk encryption. (53)
- ☐ Support for the following features on devices that connect to wireless networks should be disabled: ad hoc networks, routing between virtual private network interfaces and other network interfaces, and Internet connection sharing. (54)
- ☐ Instead of deploying a small number of wireless access points that broadcast on high power, more wireless access points that use minimal broadcast power should be deployed to achieve the desired wireless network footprint. (55)