

WIRELESS NETWORKING SECURITY

Dec 2010

© The Government of the Hong Kong Special Administrative Region

The contents of this document remain the property of, and may not be reproduced in whole or in part without the express permission of the Government of the HKSAR.

Disclaimer: Whilst the Government endeavours to ensure the accuracy of the information in this paper, no express or implied warranty is given by the Government as to the accuracy of the information. The Government of HKSAR accepts no liability for any error or omission arising from or related to the use of the information.

TABLE OF CONTENTS

Summary.....	3
I. An Introduction to Wireless Networking.....	4
Wireless Local Area Network.....	4
Access Point	4
Service Set Identifier	4
Open System Authentication.....	5
Shared Key Authentication.....	5
Ad-Hoc Mode	6
Infrastructure Mode	6
Wired Equivalent Privacy Protocol.....	6
Wi-Fi Protected Access and Wi-Fi Protected Access 2	7
II. Security Threats and Risks.....	9
"Parking Lot" Attack	9
Shared Key Authentication Flaw	10
Service Set Identifier Flaw	10
The Vulnerability of Wired Equivalent Privacy Protocol.....	11
Attack on Temporal Key Integrity Protocol (TKIP).....	12
III. Applicability of Wireless Networks for Information Processing in a Corporate Environment.....	13
IV. Best Practices in Corporate Deployment.....	15
Initialisation Phase	15

Design / Procurement Phase	16
Implementation Phase.....	18
Operations and Maintenance Phase	22
Disposition Phase	23
V. Best Practices on Using Wireless Networks	24
Tips On Configuring a Wireless Broadband router At Home	24
Tips On Internet Surfing Via Public Wireless Services	26

SUMMARY

With continual advances in technology, coupled with increasing price/performance advantages, wireless accessibility is being deployed increasingly in office and public environments. This paper discusses the security threats and risks associated with wireless networks, and outlines a number of best practices for deploying wireless networks in corporate and home environments. Finally, a set of security tips is provided for end-users surfing the Internet using public wireless networks.

I. AN INTRODUCTION TO WIRELESS NETWORKING

Wireless Internet access technology is being increasingly deployed in both office and public environments, as well as by the Internet users at home. We begin by outlining some of the basic technologies of wireless network systems.

WIRELESS LOCAL AREA NETWORK

A Wireless Local Area Network (WLAN) is a type of local area network that uses high frequency radio waves rather than wires to communicate between network-enabled devices.

ACCESS POINT

A wireless access point (AP) is a hardware device that allows wireless communication devices, such as PDAs and mobile computers, to connect to a wireless network. Usually, an AP connects to a wired network, and provides a bridge for data communication between wireless and wired devices.

SERVICE SET IDENTIFIER

A Service Set Identifier (SSID) is a configurable identification that allows wireless clients to communicate with an appropriate access point. With proper configuration, only clients with correct SSID can communicate with the access points. In effect, SSID acts as a single shared password between access points and clients.

OPEN SYSTEM AUTHENTICATION

Open System Authentication is the default authentication protocol for the 802.11 standard. It consists of a simple authentication request containing the station ID and an authentication response containing success or failure data. Upon successful authentication, both stations are considered mutually authenticated. It can be used with WEP (Wired Equivalent Privacy) protocol to provide better communication security, however it is important to note that the authentication management frames are still sent in clear text during authentication process. WEP is used only for encrypting data once the client is authenticated and associated. Any client can send its station ID in an attempt to associate with the AP. In effect, no authentication is actually done.

SHARED KEY AUTHENTICATION

Shared Key Authentication is a standard challenge and response mechanism that makes use of WEP and a shared secret key to provide authentication. Upon encrypting the challenge text with WEP using the shared secret key, the authenticating client will return the encrypted challenge text to the access point for verification. Authentication succeeds if the access point decrypts the same challenge text.

AD-HOC MODE

Ad-hoc mode is one of the networking topologies provided in the 802.11 standard. It consists of at least two wireless stations where no access point is involved in their communication. Ad-hoc mode WLANs are normally less expensive to run, as no APs are needed for their communication. However, this topology cannot scale for larger networks and lack of some security features like MAC filtering and access control.

INFRASTRUCTURE MODE

Infrastructure mode is another networking topology in the 802.11 standard, in addition to ad-hoc mode. It consists of a number of wireless stations and access points. The access points usually connect to a larger wired network. This network topology can scale to form large-scale networks with arbitrary coverage and complexity.

WIRED EQUIVALENT PRIVACY PROTOCOL

Wired Equivalent Privacy (WEP) Protocol is a basic security feature in the IEEE 802.11 standard, intended to provide confidentiality over a wireless network by encrypting information sent over the network. A key-scheduling flaw has been discovered in WEP, so it is now considered as unsecured because a WEP key can be cracked in a few minutes with the aid of automated tools. Therefore, WEP should not be used unless a more secure method is not available.

WI-FI PROTECTED ACCESS AND WI-FI PROTECTED ACCESS 2

Wi-Fi Protected Access (WPA) is a wireless security protocol designed to address and fix the known security issues in WEP. WPA provides users with a higher level of assurance that their data will remain protected by using Temporal Key Integrity Protocol (TKIP) for data encryption. 802.1x authentication has been introduced in this protocol to improve user authentication.

Wi-Fi Protected Access 2 (WPA2), based on IEEE 802.11i, is a new wireless security protocol in which only authorised users can access a wireless device, with features supporting stronger cryptography (e.g. Advanced Encryption Standard or AES), stronger authentication control (e.g. Extensible Authentication Protocol or EAP), key management, replay attack protection and data integrity.

In July 2010, a security vendor claimed they discovered vulnerability on WPA2 protocol, named "Hole 196". By exploiting the vulnerability, an internal authenticated Wi-Fi user can decrypt private data of others and inject malicious traffic into the wireless network. After investigation¹, such attack cannot actually recover, break or crack any WPA2 encryption keys (AES or TKIP). Attackers can only masquerade as AP and launch a man-in-the-middle attack when clients attached to them. Moreover, such attack would not be succeeded in a proper configured environment. If client isolation feature is enabled in access points, wireless clients are not allowed to talk with each other when they are attaching to the same access point. In this connection, attacker is unable to launch man-in-the-middle attack to other wireless users.

¹ Analysis of "Hole 196" WPA2 Attack. (<https://airheads.arubanetworks.com/article/aruba-analysis-hole-196-wpa2-attack>)

TKIP was designed to use with WPA while the stronger algorithm AES was designed to use with WPA2. Some devices may allow WPA to work with AES while some others may allow WPA2 to work with TKIP. But since November 2008, vulnerability in TKIP was uncovered where attacker may be able to decrypt small packets and inject arbitrary data into wireless network. Thus, TKIP encryption is no longer considered as a secure implementation. New deployments should consider using the stronger combination of WPA2 with AES encryption.

II. SECURITY THREATS AND RISKS

Low deployment costs make wireless networks attractive to users. However, the easy availability of inexpensive equipment also gives attackers the tools to launch attacks on the network. The design flaws in the security mechanisms of the 802.11 standard also give rise to a number of potential attacks, both passive and active. These attacks enable intruders to eavesdrop on, or tamper with, wireless transmissions.

"PARKING LOT" ATTACK

Access points emit radio signals in a circular pattern, and the signals almost always extend beyond the physical boundaries of the area they intend to cover. Signals can be intercepted outside buildings, or even through the floors in multi-storey buildings. As a result, attackers can implement a "parking lot" attack, where they actually sit in the organisation's parking lot and try to access internal hosts via the wireless network.

If a network is compromised, attacker has achieved a high level of penetration into the network. They are now through the firewall, and have the same level of network access as trusted employees within the corporation.

An attacker may also fool legitimate wireless clients into connecting to the attacker's own network by placing a unauthorised access point with a stronger signal in close proximity to wireless clients. The aim is to capture end-user passwords or other sensitive data when users attempt to log on these rogue servers.

SHARED KEY AUTHENTICATION FLAW

Shared key authentication can easily be exploited through a passive attack by eavesdropping on both the challenge and the response between the access point and the authenticating client. Such an attack is possible because the attacker can capture both the plaintext (the challenge) and the ciphertext (the response).

WEP uses the RC4 stream cipher as its encryption algorithm. A stream cipher works by generating a keystream, i.e. a sequence of pseudo-random bits, based on the shared secret key, together with an initialisation vector (IV). The keystream is then XORed against the plaintext to produce the ciphertext. An important property of a stream cipher is that if both the plaintext and the ciphertext are known, the keystream can be recovered by simply XORing the plaintext and the ciphertext together, in this case the challenge and the response. The recovered keystream can then be used by the attacker to encrypt any subsequent challenge text generated by the access point to produce a valid authentication response by XORing the two values together. As a result, the attacker can be authenticated to the access point.

SERVICE SET IDENTIFIER FLAW

Access points come with default SSIDs. If the default SSID is not changed, it is comparatively attract more attacks from attackers since these units are regarded as poorly configured devices. Besides, SSIDs are embedded in management frames that will be broadcasted in clear text regardless access point is configured to disable SSID broadcasting or enabled encryption. By conducting analysis on the captured network traffic from the air, attacker is able to obtain the network SSID and performs further attacks.

THE VULNERABILITY OF WIRED EQUIVALENT PRIVACY PROTOCOL

Data passing through a wireless LAN with WEP disabled (which is the default setting for most products) is susceptible to eavesdropping and data modification attacks. However, even when WEP is enabled, the confidentiality and integrity of wireless traffic is still at risk because a number of flaws in WEP have been revealed, which seriously undermine its claims to security. In particular, the following attacks on WEP are possible:

1. Passive attacks to decrypt traffic based on known plaintext and chosen ciphertext attacks;
2. Passive attacks to decrypt traffic based on statistical analysis on ciphertexts;
3. Active attacks to inject new traffic from unauthorised mobile stations;
4. Active attacks to modify data; or
5. Active attacks to decrypt traffic, based on tricking the access point into redirecting wireless traffic to an attacker's machine.

ATTACK ON TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)

The TKIP attack uses a mechanism similar to the WEP attack that trying to decode one byte at a time by using multiple replays and observing the response over the air. Using this mechanism, an attacker can decode small packets like ARP frames in about 15 minutes. If Quality of Service (QoS) is enabled in the network, attacker can further inject up to 15 arbitrary frames for every decrypted packet. Potential attacks include ARP poisoning, DNS manipulation and denial of services.

Although this is not a key recovery attack and it does not lead to compromise of TKIP keys or decryption of all subsequent frames, it is still a serious attack and poses risks to all TKIP implementations on both WPA and WPA2 network.

III. APPLICABILITY OF WIRELESS NETWORKS FOR INFORMATION PROCESSING IN A CORPORATE ENVIRONMENT

In recent years, the adoption of wireless networks in the corporate environment has been on the increase. Many small and medium enterprises (SMEs) have switched to wireless networks, due to the low cost of wireless devices and convenience of using such networks. Even large corporations have also considered enterprise wide deployment of wireless networks². However, convenience and flexibility come at a price; the security threat level increases with the use of wireless networks due to the inherent characteristics and weaknesses of wireless network protocols. Therefore, it is important to examine the applicability of wireless networks for information processing in a corporate environment.

As a start, the applicability of wireless networks can be defined with respect to the transmission of various categories of information. For instance, clear guidelines have been defined on the applicability of wireless networks within the Hong Kong Government. The following table summarises the applicability of wireless networks with respect to the transmission of various categories of information in accordance with the requirements specified in the Security Regulations.

Category of Information	Applicability of Using Wireless Network for Transmission
TOP SECRET	Not allowed
SECRET	Not allowed

² <http://www.entrepreneur.com/tradejournals/article/162337616.html>

CONFIDENTIAL	<p>Allowed, provided that there are sufficient authentication and transmission encryption security controls that have attained the level of encryption required for CONFIDENTIAL information.</p> <p>Use of a VPN is recommended to provide a strong authentication and encryption tunnel over a WLAN connection. In addition, proper key management and configuration policies should also be established to complement the technical solution.</p>
RESTRICTED	<p>Allowed, provided that there are sufficient authentication and transmission encryption security controls that have attained the level of encryption required for RESTRICTED information.</p> <p>The same level of encryption required for CONFIDENTIAL information is recommended, using proper key management and configuration policies similar to those for CONFIDENTIAL information.</p>
Unclassified	<p>Allowed. Following the principle that only authorised parties are permitted to access the network where information is stored, wireless networks with sufficient authentication and transmission encryption measures where appropriate are considered suitable for use by Bureaux & Departments.</p> <p>Similar to the specifications for CONFIDENTIAL and RESTRICTED information, proper key management and configuration policies should be established to complement the technical solution.</p>

IV. BEST PRACTICES IN CORPORATE DEPLOYMENT

In terms of cost effectiveness and convenience, wireless networks have gained in popularity among organisations. But new security risks come with the benefits of adopting wireless networks in an organisation. To tackle these risks effectively, various security best practices need to be considered throughout the entire deployment lifecycle. To help organisations understand at what point in their wireless network deployments a recommended security best practice might be relevant, we outline here a five-phase lifecycle model for network deployment and point out security issues that need special attention.

INITIALISATION PHASE

Determine the Business and Functional Requirements for the Use of the Wireless Network

Before designing the wireless network, it is important to understand the business and functional requirements of the wireless solution. These requirements may affect decisions on what kind of security measures should be deployed to protect the network. For example, if guest access is required, security best practices for guest access should be considered in the design stage.

Define a Wireless Security Policy

The organisation should develop a strong wireless security policy to address all the usage options of wireless networks and the types of information that can be transmitted. The policy should outline a framework for the development of installation, protection, management and usage procedures. Security and operation guidelines, standards and personnel roles should also be clearly defined.

DESIGN / PROCUREMENT PHASE

Keep Track of Development for Wi-Fi Standards

Since the 802.11 standard was first introduced, enhancements have continuously been made to strengthen data rates, signal range, and security of wireless networks. Therefore, it is a good idea to keep track of the development of new standards as they appear, in particular when procuring new equipment or acquiring new wireless network services. In any new purchase, protection by one of the stronger wireless security protocols such as WPA/AES or WPA2/AES should be considered, but by no means should such wireless security protocols be solely relied upon to protect data confidentiality and integrity, as new weaknesses in protocols may be discovered in the future.

Perform Security Risk Assessments and Audits to Identify Security Vulnerabilities

Security assessments and audits are essential means for checking the security status of a wireless network and identifying any corrective action necessary to maintain an acceptable level of security. These assessments can help identify loopholes in the wireless network, such as poorly configured access points using default or easily guessed passwords and SNMP community words, or the presence or absence of encryption. However, a security risk assessment can only give a snapshot of the risks to information systems at a given

time. As a result, it is important to perform assessments and audits regularly once the wireless network is up and running.

Perform Site Surveys

Due to the nature of radio frequency (RF) propagation, radio signal emissions cannot generally be contained within a particular building or location. Excessive coverage by the wireless signal could pose significant threat to the organisation, opening it to parking lot attacks on the network. Therefore, it is necessary to have a good understanding of the coverage requirements for the desired wireless network during the network-planning phase. By performing a site survey, one can identify:

1. the appropriate technologies to apply;
2. obstacles to avoid, eliminate, or work around;
3. coverage patterns to adopt; and
4. amount of capacity needed.

Apply a Defence-in-Depth Approach

The concept of “defence-in-depth” has been widely employed in the secure design of wired networks. The same concept can also be applied to wireless networks. By implementing multiple layers of security, the risk of intrusion via a wireless network is greatly reduced. If an attacker breaches one measure, additional measures and layers of security remain in place to protect the network.

Separation of wireless and wired network segments, use of strong device and user authentication methods, application of network filtering based on addresses and protocols,

and deployment of intrusion detection systems on the wireless and wired networks are all possible measures that can be employed to build multiple layers of defence.

Separate Wireless Networks from Wired Networks

Due to the nature of wireless technology, wireless networks are relatively hard to contain within a building and it is generally considered to be an un-trusted network. As a best practice, wireless networks and wired networks should not be directly connected to each other. It is common to deploy firewalls to separate and control the traffic between different networks. For example, ARP broadcast packets should be blocked from entering a wired network from a wireless network since a malicious user could uncover internal information, such as Ethernet MAC address from these broadcasts.

Segment the Access Point's Coverage Areas

Due to the limited transmission capacity of a wireless network, a malicious attacker can easily launch a Denial-of-Service (DoS) attack to bring down the network. Segmenting access point coverage areas can balance the loads on a wireless network and minimise any impact from DoS attacks.

IMPLEMENTATION PHASE

Implement Strong Physical Security Controls

The loss or theft of network equipment may pose a significant threat to a wireless network because configuration of the network can be retrieved from a lost access point or wireless interface card. By securely mounting network equipment, such as access points, in less accessible locations together with strong physical security controls, the risk of theft can be minimised.

Avoid Excessive Coverage of Wireless Networks

Using the information collected during the site survey, proper placement of access points can be designed to avoid excessive coverage by the wireless network and hence limit the possibility of intrusion. In addition to proper placement of the access points, adjusting the radio frequency (RF) power transmission or using directional antennas can also control the propagation of the RF signal and hence control coverage of a wireless network.

Secure Access Points

Access points are the core of a wireless network. Their security clearly has an overall effect on the security of the wireless network. Properly securing access points is the first step in protecting a wireless network. The following suggestions can help in hardening access points:

1. Change the default configuration settings;
2. Change encryption keys regularly;
3. Ensure that all access points have strong, unique administrative passwords and change the passwords regularly;
4. Disable all insecure and unused management protocols on access points and configure the remaining management protocols for least privilege;

5. Activate logging features and direct all log entries to a remote logging server;
6. Enable wireless threshold parameters, such as inactivity timeouts and maximum supported associations.

Use Non-suggestive Service Set Identifier (SSID) Naming Conventions

In a wireless network, an SSID serves as a network name for segmenting networks. A client station must be configured with the correct SSID in order to join a network. The SSID value is broadcast in beacons, probe requests and probe responses. To prevent a malicious attacker from collecting reconnaissance information on a wireless network by eavesdropping, SSIDs should not reflect internal information of the organisation.

Disable Direct Client-to-Client “Ad-Hoc Mode” Transmissions

In general, a wireless network can be operated using three different topologies; infrastructure mode, ad-hoc mode and bridging mode. When a wireless network operates in ad-hoc mode, client stations are connected directly and no access point is required. Using this mode, a potential attacker can gain access to a client station easily if the client station is improperly configured. Unless there is a specific business need, the ad-hoc mode should be disabled on wireless devices.

Limit Client-to-Client Communication through the Access Point

Most installed wireless networks operate in “infrastructure” mode that requires the use of one or more access points. With this configuration, all traffic in the wireless network travels through the access points. By controlling the communication among client stations

at the access points, malicious users can be prevented from gaining access to vulnerable client stations.

Keep Security Patches Up-to-date

Newly discovered security vulnerabilities in vendor products should be patched to prevent inadvertent and malicious exploits. Patches should also be tested before deployment so as to ensure they work correctly.

Employ MAC Address Filtering on Access Points

MAC address filtering can be considered the first layer of defence for wireless networks. With MAC address filtering enabled, only devices with pre-approved MAC addresses can see the network and be granted access to the network. However, such access control should by no means be solely relied upon to protect data confidentiality and integrity, as tools are available on the Internet for modifying the MAC address of a client. Besides, MAC address filtering mechanisms may not be feasible in some scenarios such as the implementation of public wireless hotspots.

Deploy Wireless Intrusion Detection Systems

Deploying wireless intrusion detection systems on the network can help detect and respond to malicious activities in a timely manner. More recently, a number of wireless intrusion detection systems have been equipped with capabilities to detect and prevent rogue access points.

OPERATIONS AND MAINTENANCE PHASE

Educate Users about the Risks of Wireless Technology

User awareness is always a critical success factor in effective information security. A good policy is not enough. It is also important to educate all users in following the policy. Best practices or security guidelines should be developed that end-users understand and adhere to.

Keep an Accurate Inventory of All Wireless Devices

An accurate inventory of all authorised wireless devices helps identify rogue access points during security audits. This inventory will also be helpful for a variety of support tasks.

Publish a Coverage Map of the Wireless Network

Network administrators should develop a coverage map of the wireless network, including locations of respective access points and SSID information. This map is a valuable asset for troubleshooting, or handling a security incident.

Develop Security Configuration Standards for Access Point

To simplify daily operations and ensure all access points are protected with appropriate measures, it is recommended a baseline security configuration standard for access points be developed. It is not uncommon to see security settings restored to their default factory

settings after an access point is reset, which usually occurs when the access point experiences an operational failure. If a baseline security configuration standard is available, appropriate personnel can simply follow the standard settings to re-configure the access point.

Review Audit Logs Regularly

Regular checking of log records must be performed, to ensure the completeness and integrity of all logs. Any irregularities spotted must be reported and a detailed investigation should be carried out if necessary.

Develop Incident Response Procedures

It is recommended that administrators develop a set of in-house procedures for incident response, and update these procedures from time to time to address new potential security threats.

DISPOSITION PHASE

Remove All Sensitive Configuration Information before Disposal

During disposal of wireless components, it is important to erase all sensitive configuration information, such as pre-shared keys and passwords, on the devices that are being disposed of. Malicious users might make use of the configuration information to conduct subsequent attacks on the network. Manual removal of configuration settings through the

management interface is a must prior to disposal. Organisations may also consider degaussing devices whenever feasible. Secure deletion utilities can also be used if devices have storage disks.

V. BEST PRACTICES ON USING WIRELESS NETWORKS

TIPS ON CONFIGURING A WIRELESS BROADBAND ROUTER AT HOME

How Do I Select My Wireless Network Mode?

In general, a wireless network can be operated using three different topologies; infrastructure mode, ad-hoc mode and bridging mode. When a wireless network operates in ad-hoc mode, client stations are connected directly and no access point is required. Using this mode, a potential attacker can gain access to a client station easily if the client station is improperly configured. Unless there is a specific business need, the ad-hoc mode should be disabled on wireless devices.

How Do I Locate My Wireless Broadband Router Securely?

1. Avoid placing the router against an outside wall or window, or against a common wall with an adjacent home to ensure that the signal does not extend beyond the required area.
2. To ensure that unauthorised people cannot tamper with your router, try to place it in a physically secure location.
3. Some routers allow you to reduce the output power of the device. To minimise leakage outside the coverage area the wireless network is meant to service,

turn down the broadcast power, if possible. This is one way to prevent too strong a signal from extending beyond the desired wireless broadcast area and being accessible to the “outside” world.

How to Configure My Wireless Broadband Router Securely?

User name and Password

Change the default user name and password because they are often easily guessed. Some manufacturers might not allow you to change the username, but at least the password should be changed.

Encryption (WEP/WPA/WPA2)

Whenever possible, WEP should be avoided. Instead, use WPA2/AES or WPA/AES if it is supported on the device.

Authentication Type (Open Authentication or Shared Key Authentication)

The shared key mechanism should never be used. Instead, a stronger mutual authentication as defined in the 802.11i standard should be considered.

Wireless Network Name / SSID

The default SSID should be changed. The new SSID should not be named to refer the network products being used, reflect your name or other personal information, otherwise the information could aid an attacker in collecting reconnaissance information about you and your wireless network.

Broadcast Network Name / SSID

Users may consider disabling SSID broadcasting or increasing the “Beacon Interval” to the maximum. Suppress SSID broadcasting could not prevent sophisticated attackers to steal SSID by sniffing the management frames between the communication of access points and clients, however it could be able to stop casual wireless clients from discovering the wireless network or attempting to access.

MAC Address Filtering

Enabling MAC address filtering is recommended as another layer of protection.

Dynamic Host Configuration Protocol (DHCP)

Disabling the DHCP feature, if possible, is recommended, as DHCP makes it easier for malicious attackers to access a wireless network.

TIPS ON INTERNET SURFING VIA PUBLIC WIRELESS SERVICES

Once you have a wireless device such as a notebook computer or a hand-held device connected to public wireless hotspots, you are exposing yourself to potential attacks from remote attackers. Nonetheless, the following security tips may prevent you from falling into the traps laid by attackers:

1. Don't leave your wireless device unattended;
2. Protect Your Device With Passwords: Enable your device's power-on login, system login authentication, and password-protected screen saver.
3. Disable Wireless Connection When It Is Not In Use: Wi-Fi, infrared, and Bluetooth devices are constantly announcing their presence if they are enabled.

That means they are waving hands to attackers, even though you may be unaware of it.

4. **Keep Your Wireless Network Interface Card Drivers Up-to-date:** A network interface card driver is just a piece of software. It is not immune to software bugs. Keeping the drivers up-to-date assures that wireless devices have the latest protection and support from product vendors.
5. **Protect your device with anti-virus software using the latest virus definitions.** This can minimise the risk of infection by computer viruses or spyware.
6. **Encrypt Sensitive / Personal Data on the Device:** Even when an unauthorised user gains access to your device, encryption will keep your data away from an opportunistic thief.
7. **Turn off Resource Sharing Protocols for Your Wireless Interface Card:** When you share files and folders, your shared resources may attract attackers attempting to manipulate them.
8. **Remove Your Preferred Network List When Using Public Wireless Service:** Some operating systems offer a feature for you to build your own list of preferred wireless networks. Once you have this list defined, your system will keep searching for a preferred network and try to connect to the preferred network automatically. By capturing this information sent out from your system, an attacker could set up a fake wireless access point, which meets the settings of a wireless network on your Preferred Network List. In doing so, your device would automatically connect to the attacker's fake wireless network.
9. **Turn off Ad-Hoc Mode Networking:** "Ad-hoc" mode networking enables your wireless device to communicate with other computers or devices through a wireless connection directly with minimal security against unauthorised incoming connections. This should be disabled to prevent attackers from easily gaining access to information and resources on your device.

10. **Do Not Enable Both Wireless and Wired Network Interface Cards at the Same Time:** When a device is connected to a wired LAN with the wireless network interface card still enabled, there is a possibility that attackers can sneak into the wired LAN through an open wireless network if network bridging is enabled.
11. **Check the Authenticity of a Captive Portal:** Captive portal web pages are commonly used in public hotspots as a means of user authentication and for deterrent protection. When connecting to a public hotspot, the user will be redirected to a captive portal page. However, attackers could also set up fake captive portals to harvest personal information. Therefore, when using public hotspots, it is important to check the authenticity of a captive portal by verifying the server certificate from the website.
12. **Don't Send Sensitive / Personal Information When Using Public Wireless Networks:** Public wireless networks are generally considered to be insecure. You should not transmit sensitive or personal information over a public hotspot without proper security controls.
13. **Encrypt Your Wireless Traffic Using a Virtual Private Network (VPN):** If transmission of sensitive or personal information over a public wireless network is unavoidable, a VPN solution can help ensure the confidentiality of communications using cryptographic technologies. If you want to learn more about VPN technologies, please refer to the paper on "Virtual Private Network Security".
14. **Disable Split Tunnelling When Using VPN:** It is possible to connect to the Internet or other insecure networks while at the same time holding a VPN connection to a private network using split tunnelling, but this may pose a risk to the connecting private network.
15. **Remove All Sensitive Configuration Information Before Disposal:** If you are disposing old wireless components, it is important to erase all sensitive

configuration information, such as Service Set Identifiers (SSIDs) or encryption keys, on the devices to be disposed of.

Though there are a number of other security measures you can take, these security tips provide a good start for protecting wireless devices and your personal information when connecting to a public wireless networks.