

Wireless Security – Information for CIOs

The purpose of this paper is to make you aware of possible vulnerabilities in your wireless systems and how you might go about mitigating such risks. It includes suggested management, operational and technical countermeasures. The paper has been developed by the IT Security Expert Advisory group (ITSEAG) which is part of the Trusted Information Sharing Network for critical infrastructure protection (TISN).¹

Introduction

Does your organisation use wireless technologies? If yes, do you have a strategy for managing these technologies? How is wireless technology being used in your organisation and how does it operate? Who has access to it? Do you know how your wireless capabilities interact with other IT systems? Are wireless applications becoming critical to the operation of your business? How would any degradation of your wireless services impact on the bottom line? These are just some of the questions that you need to have answered in an environment where these new technologies are being more widely deployed.

Organisations and users are increasingly looking for systems that provide higher productivity and cost savings. In light of this many organisations have embraced wireless technologies that not only provide convenience and flexibility of use, but also deliver cost savings. As a result in recent years the application of wireless technologies in home and business networking solutions has seen significant growth.

Due to the benefits offered by wireless technologies they are now being used to control critical infrastructures such as railway networks, energy transmission and other utilities.

¹ TISN enables the owners and operators of critical infrastructure to share information on important issues. It is made up of a number of sector-specific Infrastructure Assurance Advisory Groups (IAAG), several Expert Advisory Groups (EAG), and the Critical Infrastructure Advisory Council (CIAC - which is the peak body of TISN and oversees the IAAGs and the EAGs). **More information on TISN can be sought from <http://www.tisn.gov.au> or by contacting cip@ag.gov.au.** The ITSEAG is one of the expert advisory groups within the TISN framework. The ITSEAG provides advice to the CIAC and the sector-based IAAGs on IT issues as they relate to critical infrastructure protection. It is made up of academic specialists, vendors, consultants and some industry association representatives who are leaders in the information technology/e-security field. **The ITSEAG Secretariat can be contacted on (02) 6271 1426.**

DISCLAIMER: To the extent permitted by law, this document is provided without any liability or warranty. Accordingly it is to be used only for the purposes specified and the reliability of any assessment or evaluation arising from it are matters for the independent judgement of users. The document is intended as a general guide only and users should seek professional advice as to their specific risks and needs.

Whilst there are several advantages of wireless technologies there are also many risks associated with them. Wireless networks are exposed to many of the same risks as wired networks, but they are also vulnerable to additional risks. Wireless networks transmit data through radio frequencies, and are open to intruders unless protected. Intruders have exploited this openness to access systems, destroy or steal data, and launch attacks that tie up network bandwidth and deny service to authorized users.²

This paper should not be taken as an exhaustive list of vulnerabilities or risks associated with these technologies. It mainly deals with the IEEE 802.11 group of standards for Wireless Local Area Networks (WLANs), since these are the most widely used in the critical infrastructure sectors.

Overview of Wireless Technologies

As mentioned above wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling. Wireless technologies use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables. Wireless technologies range from complex systems, such as Wireless Local Area Networks (WLAN) and cell phones to simple devices such as wireless headphones, microphones, and other devices that do not process or store information. They also include infrared (IR) devices such as remote controls, some cordless computer keyboards and mice, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver to close the link.

Wireless networks serve as the transport mechanism between devices and among devices and the traditional wired networks (enterprise networks and the Internet). Wireless networks are many and diverse but are frequently categorized into four groups based on their coverage range: Wireless Wide Area Networks (WWAN); Wireless Metropolitan Area Network (WMAN); Wireless Local Area Network (WLANs), and Wireless Personal Area Networks (WPAN). WWAN includes wide coverage area technologies such as 2G cellular, Cellular Digital Packet Data (CDPD), Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS) and Mobitex. WMAN represents wireless internet connection at broadband speeds within city or suburbs, it includes 802.16. WLAN, representing wireless local area networks, includes 802.11, HiperLAN, and several others. WPAN, represents wireless personal area network technologies such as Bluetooth and IR.

² Page 1 Security for Wireless Networks and Devices, Shirley Raddock, National Institute of Standards and Technology <http://www.itl.nist.gov/lab/bulletns/bltnmar03.htm>.

Wireless Technologies and Standards

There are a number of standards used in wireless technologies. Some of the key ones include:

- The IEEE 802.11 standards provide specifications for high-speed networks that support most of today's applications. The IEEE 802.11 specifications are wireless standards that specify an "over-the-air" interface between a wireless client and a base station or access point, as well as among wireless clients. These 802.11 standards can be compared to the IEEE 802.3 standard for Ethernet for wired LANs. The IEEE 802.11 specifications address both the Physical (PHY) and Media Access Control (MAC) layers and are tailored to resolve compatibility issues between manufacturers of Wireless LAN equipment.
- IEEE802.15 provides standards for low complexity and low-power consumption connectivity.
- IEEE 802.16 standard, the "Air Interface for Fixed Broadband Wireless Access Systems" is also known as the IEEE WirelessMAN air interface. This technology is designed to provide wireless last-mile broadband access in the Metropolitan Area Network (MAN), delivering performance comparable to traditional cable, DSL, or T1 offerings.
- Bluetooth (Wireless Personal Area Network) is an alternative wireless network technology that has followed a different development path than the 802.11 family. Bluetooth supports a very short range (approximately 10 meters) and relatively low bandwidth (1 Mbps). In practice, Bluetooth networks PDAs or cell phones with PCs but does not offer much value for general-purpose WLAN networking. The Bluetooth standard was developed by a computer and communications industry consortium, specifying how mobile phones, computers, and PDAs interconnect with each other, with home and business phones, and with computers using short-range wireless connections.
- IEEE 802.1X offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1X ties a protocol called EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication.

This list of standards is in no way comprehensive. There are several standards within IEEE 802.11 ranging from IEEE 802.11a to IEEE 802.11j and IEEE 802.11R. There are also three additional standards within the IEEE 802.11 protocol on which work has commenced; these include IEEE 802.11j, 802.11k and 802.11m. The paper does not go into the detail of each of the standards within the IEEE 802.11 family but in general terms stipulates the concerns/risks/vulnerabilities within this group of standards and some ways to manage them.

It is also important to note that this paper does not focus on other WLAN standards besides IEEE 802.11 such as the European Telecommunications Standards Institute's (ETSI) HiperLan and the HomeRF standard for the home user and small businesses.

Security Features of IEEE 802.11

The IEEE 802.11 WLAN – or WiFi specification has identified several services to provide a secure operating environment. The security services are provided largely by the Wired Equivalent Privacy (WEP) protocol to protect link level data during wireless transmission between clients and access points. WEP does not provide end-to-end security, but only for the wireless portion of the connection³. However, there are a number of problems with the WEP protocol and its vulnerabilities significantly limit its ability to safeguard data. Commonly available tools such as AirSnort, WEPCrack and dweputils have the ability to crack WEP keys by analysing traffic from totally passive data captures⁴. An improvement on WEP is the Wi-Fi Protected Access (WPA) which was introduced in 2003. WPA avoids most of WEP's vulnerabilities.

However, the above vulnerabilities don't make WEP unusable; one just has to be careful about how and when it is used.

³ Page3-13 NIST, Special Publication 800-48, Wireless Network Security, 802.11, Bluetooth and Handheld Devices, Tom Karygiannis and Les Owens

⁴ WEP Vulnerabilities—Wired Equivalent Privacy, Lee Barken,
<http://www.informit.com/articles/article.asp?p=102230&seqNum=12>

WLAN security checklist*

Brian Clark, 11 Feb 2003

WLANs are vulnerable and it is a good idea to follow a few simple tips to better protect your WLAN. Hackers are smart too but when your WLAN is protected they very well may get frustrated and give up. The Checklist:

- DO NOT allow SMTP relay.
- DO use SMTP authentication.
- Get a Firewall/NAT router
- Secure all user accounts with hard to guess passwords.
- Monitor your network traffic and block unknown IP/ranges.
- If you use a VPN - secure it too.
- Backup all data!
- Use http authorization to get to the Internet. Some proxy servers support this. Use a stateful packet inspection firewall.
- Update A/V definitions daily if possible.
- If you need better than normal authentication, try using an RSA SecurID solution, smart cards, or similar.

* This is a suggested checklist only. Organisations should have their own checklist tailored to their business needs

The three basic security services defined by IEEE for the WLAN environment are:

- **Authentication**—A primary goal of WEP was to provide a security service to verify the identity of communicating client stations. This provides access control to the network by denying access to client stations that cannot authenticate properly. This service addresses the question, “Are only authorized persons allowed to gain access to my network?”
- **Confidentiality**—Confidentiality, or privacy, was a second goal of WEP. It was developed to provide “privacy achieved by a wired network.” The intent was to prevent information compromise from casual eavesdropping (passive attack). This service, in general, addresses the question, “Are only authorized persons allowed to view my data?”
- **Integrity**—Another goal of WEP was a security service developed to ensure that messages were not modified in transit between the wireless clients and the access point in an active attack. This service addresses the question, “Is the data coming into or exiting the network trustworthy—has it been tampered with?”

Threats

There have been many reports describing attacks on 802.11 wireless networks that expose organisations to security risks. These attacks, either active or passive, are essentially on confidentiality, integrity and network availability.

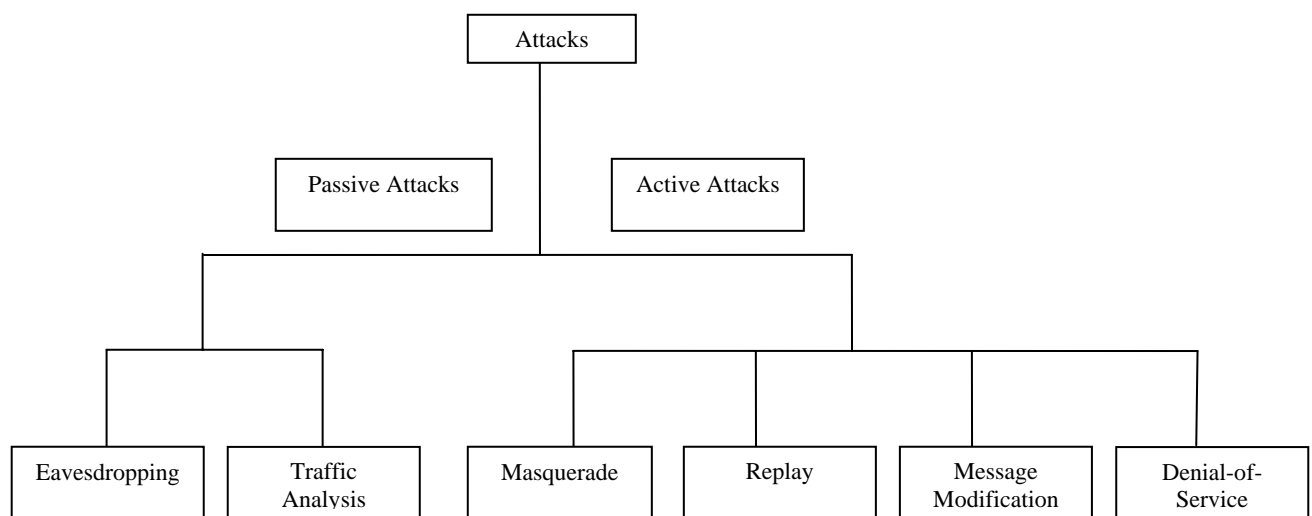


Figure1 Taxonomy of Security Attacks

According to the US National Institute of Standards and Technology (NIST) there are six different types of attacks under passive and active categories against IEEE 802.11⁵ networks:

- **Passive Attack**—An attack in which an unauthorized party gains access to an asset and does not modify its content (i.e. eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described below:
 - **Eavesdropping**—The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a LAN between two workstations or tuning into transmissions between a wireless handset and a base station.

⁵ Page 3-20 NIST, Special Publication 800-48, Wireless Network Security, 802.11, Bluetooth and Handheld Devices, Tom Karygiannis and Les Owens

- **Traffic analysis**—The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.
- **Active Attack**—An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable. Active attacks may take the form of one of four types (or combination thereof): masquerading, replay, message modification, and denial-of-service (DoS). These attacks are defined below:
 - **Masquerading**—The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.
 - **Replay**—The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.
 - **Message modification**—The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
 - **Denial-of-service**—The attacker prevents or prohibits the normal use or management of communications facilities.

Gartner Says Wireless LANs are the Major Wireless Security Problem Facing Businesses Through 2008

Analysts Discuss How to Secure a Wireless Network at Gartner IT Security Summit 2004

WASHINGTON, D.C., June 9, 2004 — Through 2006, 70 percent of successful wireless local area network (WLAN) attacks will be because of the misconfiguration of WLAN access points (AP) and client software, according to Gartner, Inc. Security for WLANs and personal digital assistants (PDAs) in the company needs to be driven by updated security policies that address the unique demands of the mobile workplace.

Gartner presented these findings today during the Gartner IT Security Summit 2004, which is taking place here, through June 9.

"Whether hackers are able to enter a company's WLAN through an unprotected AP or through a peer workstation, once they are associated with the network, they will be difficult to detect because they may not be visible in or near the network site," said John Pescatore, vice president and Gartner fellow. "A clever hacker will play it safe and use the company's resources quietly, and as a result, may never be found."

To protect themselves, businesses must make sure that employees or hackers don't install unauthorized wireless APs on the network and that APs are configured securely. In dense environments, such as urban areas or multi-tenant office buildings, companies have to make sure that their users don't connect to other companies' networks.

The least expensive, and least effective, way of doing this is to buy a wireless sniffer handheld and walk the perimeter of the network. The most expensive, and most secure, is to install a separate set of wireless intrusion detection sensors.

"Businesses should use sniffers to demonstrate potential exposure problems to management, especially to the management that funds security problems," Pescatore said. "Sniffer walks should not be attempted as an ongoing survey method, but should be kept on standby. If rogue WLAN activity is detected by network monitoring systems, individual members of the IT staff can be dispatched, to act as trackers, to hone in on unauthorized signal sources."

Gartner says that companies will get the most efficient WLAN intrusion detection protection from a vendor-independent dedicated sensor investment. The overwhelming advantage of this method is that all WLAN traffic can be detected regardless of the equipment and vendors involved.

Security Countermeasures for Wireless Networks

NIST has suggested countermeasures at the management, technical and operational level for securing wireless networks. These include:⁶

- ***Management Countermeasures***

According to NIST, management countermeasures for securing wireless networks begin with a comprehensive security policy. A security policy, and compliance

⁶ Page 3-22 NIST, Special Publication 800-48, Wireless Network Security, 802.11, Bluetooth and Handheld Devices, Tom Karygiannis and Les Owens.

therewith, is the foundation on which other countermeasures—operational and technical—are rationalized and implemented. A WLAN security policy should be able to do the following:

- Identify who may use WLAN technology in an agency
- Identify whether Internet access is required
- Describe who can install access points and other wireless equipment
- Provide limitations on the location of and physical security for access points
- Describe the type of information that may be sent over wireless links
- Describe conditions under which wireless devices are allowed
- Define standard security settings for access points
- Describe limitations on how the wireless device may be used, such as location
- Describe the hardware and software configuration of all wireless devices
- Provide guidelines on reporting losses of wireless devices and security incidents
- Provide guidelines for the protection of wireless clients to minimize/reduce theft
- Provide guidelines on the use of encryption and key management
- Define the frequency and scope of security assessments to include access point discovery.

Agencies should institute security manuals which include established procedures, (before an attack), and procedures to handle in the event of an attack. It may also contain security policies, response team, etc.

Agencies should also ensure that all critical personnel are properly trained on the use of wireless technology. Network administrators need to be fully aware of the security risks that WLANs and devices pose. They must work to ensure security policy compliance and to know what steps to take in the event of an attack. Finally, the most important countermeasures are trained and aware users.

- ***Operational Countermeasures***

Physical security is the most fundamental step for ensuring that only authorized users have access to wireless computer equipment. Physical security combines such measures as access controls, personnel identification, and external boundary protection. As with facilities housing wired networks, facilities supporting wireless networks need physical access controls. For example, photo identification, card badge

readers, or biometric devices can be used to minimize the risk of improper penetration of facilities. External boundary protection can include locking doors and installing video cameras for surveillance around the perimeter of a site to discourage unauthorized access to wireless networking components such as wireless access points (APs). In addition, agencies should use wireless security assessment tools (e.g. vulnerability assessment) and regularly conduct scheduled security audits.

- ***Technical Countermeasures***

Technical countermeasures involve the use of hardware and software solutions to help secure the wireless environment. Software countermeasures include proper Access Point (AP) configurations (i.e. the operational and security settings on an AP), software patches and upgrades, authentication, intrusion detection systems (IDS), personal firewalls for wireless devices and encryption. Hardware solutions include smart cards, virtual private networks (VPNs), public key infrastructure (PKI), a separate switching infrastructure for the wireless network (separating it from a wired network) and biometrics. It should be noted that hardware solutions, which generally have software components, are listed simply as hardware solutions. Additionally, due to the mobile nature of wireless networks, hard disk encryption is also highly recommended or mandatory.

Questions You Should Ask

In light of what has been discussed above, it is important that you have mechanisms in place to protect your wireless applications. Following are some questions that you might ask yourself to ensure that the use of wireless technologies in your organisation is well protected:

- Are we using wireless technologies? Where are we deploying these technologies?
- How critical are they to our business? Is there a trend towards more of our critical data being carried over wireless?
- Do we have a wireless security policy in place incorporating appropriate management, operational and technical countermeasures? How recently was it reviewed? (This should be reviewed once every 12 months at the least, preferably more frequently due to fast pace of development in wireless access technology.)

And if you want to get technical...

- Do we check where, physically, our wireless network is accessible from?

- Do we have a register of access points and wireless network interface cards (NICs)?
- Do we regularly check for rogue access points?
- Does our service set identifier (SSID) in anyway identify us?⁷
- Do our wireless enabled computers utilise a virtual private network (VPN)?

Conclusion

It is essential that organisations have suitable protective measures for their IT systems particularly where wireless technologies are used. The wireless group of standards IEEE 802.11, although not foolproof, do provide basic security as do the security countermeasures promoted by NIST. Implementing these will mitigate the risks associated with the use of wireless technologies and save your organisation from potentially costly attacks.

Further Information

Further information on wireless technologies and their security can be found at:

<http://standards.ieee.org/wireless/index.html>

This is the website for the IEEE standards. It provides information on the wireless IEEE standards and helps to answer questions on the IEEE wireless standards initiative. It also provides links to the various working groups on the IEEE standards.

<http://csrc.nist.gov/>

This is the website for NIST's Computer Security Research Centre. It provides a link to the NIST document (referenced in this paper) "Wireless Network Security 802.11, Bluetooth and Handheld Devices" by Tom Karygiannis and Les Owens. This paper will help you to understand the security issues pertaining to wireless technologies such as IEEE 802.1 and Bluetooth and provides some strategies that you can put in place to protect your wireless applications.

⁷ SSID is a sequence of characters that uniquely names a wireless local area network.

<http://www.nwfusion.com/news/tech/2002/0325tech.html>

This provides a link to the article “802.1X provides user authentication” by Paul Goransson, Network World Fusion, 24 March 2002. This article will help you to understand the capabilities of the 802.1X standard

<http://insight.zdnet.co.uk/communications/wireless/0,39020430,2132483,00.htm>

This provides a link to the article “A to Z of Wireless Standards” by Rupert Goodwins, ZDNet UK, 26 March 2003. It provides a guide to the IEEE 802.11 family of standards.

http://www.firstmonday.dk/issues/issue8_8/critical/#c2

This provides a link to the paper “A Social Ecology of Wireless Technology” by Critical Friends of Technology. This paper looks at both costs and risks of wireless technologies, employing a holistic framework for evaluating technological impacts.

<http://nc3ta.nc3a.nato.int/vol2-sup2/ch02s02.html>

This provides a link to the paper “2.2. Wireless Networking - 802.11 Standards” by The NATO C3 Technical Architecture. This paper provides a guide to the IEEE 802.11 family of standards.

<http://www.itl.nist.gov/lab/bulletns/bltnmar03.htm>

This provides a link to the NIST Paper “Security For Wireless Networks And Devices” by Shirley Radack. The paper provides a snapshot of security issues associated with wireless technologies.