WIRELESS SECURITY—INFORMATION FOR CIOS—TECHNICAL APPENDIX

Introduction

This appendix provides Chief Information Officers (CIOs), Chief Technology Officers (CTOs) and IT managers with technical detail to support the primary reports on the topic of Wireless Security. The appendix concentrates on the WiFi and WiMAX technologies, detailing the threats and risks in these technologies and ways to manage them. The paper includes additional information regarding management, operational and technical countermeasures to the standard CIO paper, to help organise related decisions.

This technical appendix and the associated reports have been developed by the IT Security Expert Advisory Group (ITSEAG) which is part of the Trusted Information Sharing Network (TISN) [1] for critical infrastructure protection.

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 (RF) so there is an increased chance that communications may be tapped into by intruders unless properly protected. Intruders have exploited the openness of wireless systems to access systems, destroy or steal data, launch attacks that tie up network bandwidth and deny service to authorised users, and to eavesdrop on conversations[2]. For example, attackers have compromised wireless systems to gain access to sensitive payment card data.

This paper should not be taken as an exhaustive technical coverage of vulnerabilities or risks associated with wireless technologies. It primarily deals with the IEEE 802.11

---

[1] TISN enables the owners and operators of critical infrastructure to share information on important issues. It is made up of nine 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 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 security 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 7018.

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

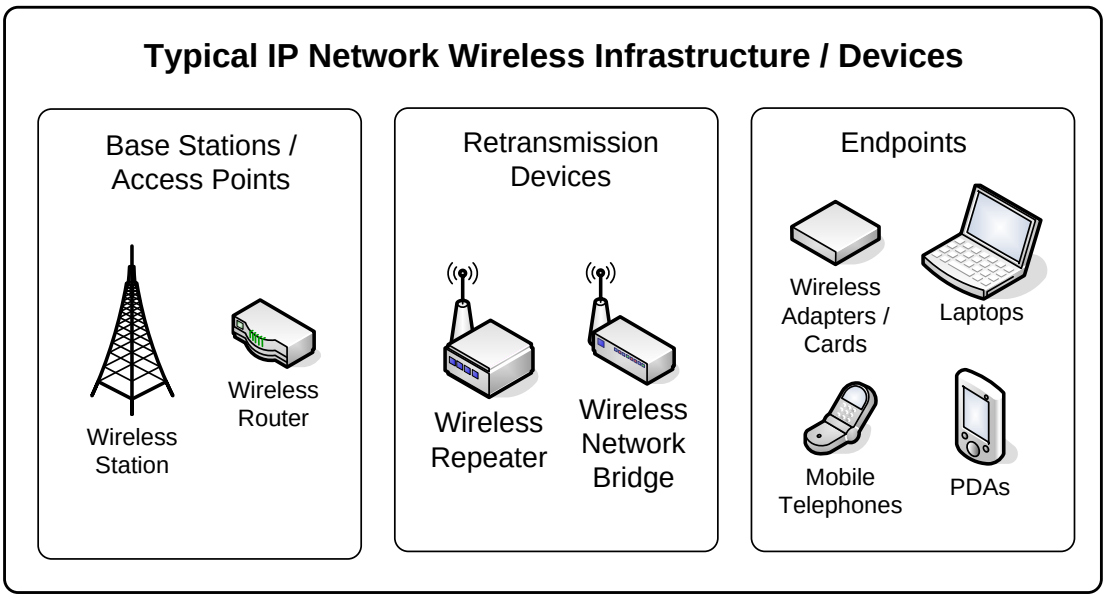
Revised June 2008

group of standards for Wireless Local Area Networks (WLANs) and the IEEE 802.16 group of standards for Wireless Metropolitan Area Networks (WMANs).

Overview of wireless technologies

Wireless technologies enable devices to communicate without physical connections, that is, without requiring network or peripheral cabling. Instead, wireless technologies use RF transmissions to transmit data 'over the air'.

Wireless technologies range from complex systems, such as local area networking and mobile phone networks (including 3G mobile phones[3]), to simple devices such as wireless headphones, microphones and other devices that do not process or store information and generally use short-range protocols such as Infrared or Bluetooth for communications.



Infrared (IR) devices, such as remote controls, cordless computer keyboards and mice, all require a direct line of sight between the transmitter and the receiver to complete the link. While Bluetooth has largely replaced IR for short-range connectivity, many legacy and existing devices continue to have IR technology available.

Laser and microwave links are less common wireless communication technologies that are most commonly utilised for inter-building LAN connectivity and multimedia connections.

Classification of wireless networks

Wireless networks serve as a data transport mechanism between other wireless communications and the traditional wired networks. Wireless networks can be structured differently but are frequently categorised into four main groups based on their coverage range:

[3] Next generation (3G) wireless networks are not IEEE 802.11 networks. Rather, they are networks dedicated to personal devices, including PDAs and cellular telephones.

Wireless class	Example technologies	Range	Example uses/applicability
Wireless wide area network (WWAN)	3G, 2G, GPRS, CDMA, Ev-DO	10 km +	Used for high mobility applications that do not require large bandwidth, such as mobile telephone internet services.
Wireless metropolitan area network (WMAN)	WiMAX, Mobile Broadband Wireless Access	1 km to 10 km	Offers high data speeds and significant range. WMAN technologies are utilised primarily as wireless broadband links, such as for inter-building connections.
Wireless local area network (WLAN)	WiFi, HiperLAN	Up to 1 km	Used for applications that require high bandwidth connections at low range, such as wireless access for laptops to a corporate network from within the company's offices, or to access Internet 'hot spots' at airports, cafes, and other locations.
Wireless personal area network (WPAN)	Bluetooth, Infrared, ZigBee, UWB	Up to 100 m	Used for small devices that only require low bandwidth and little range, such as Bluetooth headsets for mobile phones.

- **Wireless wide area network (WWAN)**—includes wide coverage area technologies such as 2G cellular (including General Packet Radio Service (GPRS) and 3G cellular (including High Speed Packet Access (HSPA)).
- **Wireless metropolitan area network (WMAN)**—represents wireless Internet connection at broadband speeds within cities or suburbs and is often referred to as wireless broadband. It includes technologies such as those specified in IEEE 802.16 (WiMAX) and emerging standards such as Mobile Broadband Wireless Access (MBWA) 802.20. In particular, WiMAX (an implementation of IEEE 802.16) has been adopted in rural areas and developing economies, such as Africa, where traditional telecommunications infrastructure has not previously been deployed[4].
- **Wireless local area network (WLAN)**—includes Wi-Fi (802.11) and HiperLAN (European version of Wi-Fi), and is a type of local-area network in which data is sent and received via high-frequency radio waves rather than cables or wires.
- **Wireless personal area network (WPAN)**—represents wireless personal area network technologies such as Bluetooth (802.15), Infrared, ZigBee and Ultra Wideband (UWB) technologies.

[4] WiMAX / BWA in Africa, Adlane Fellah, www.wimax.com/commentary/spotlight/wimaxspotlight2005_06_15_part1

Figure 1 illustrates the range and data rates of the above wireless technologies.

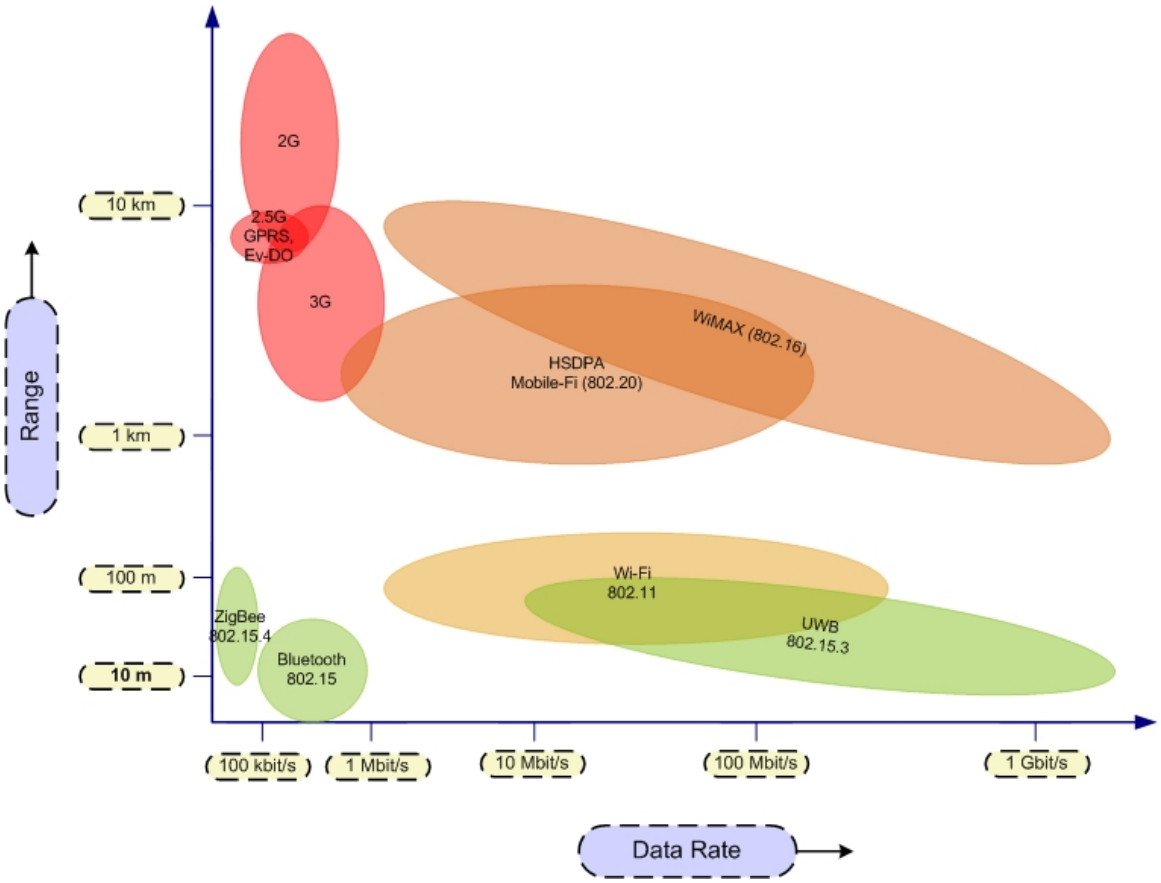


Figure 1: Wireless technologies vs data rates
Adapted from: Wireless Communications - The Future by William Webb

Wireless technologies and standards

There are a number of standards used in wireless technologies. Key standards include:

Wireless specification standards

- The IEEE 802.15 standard is often referred to as 'Bluetooth'. This standard defines a low complexity and low power connection, ideal for close range devices (typically from 10 to 100 metres) and relatively low transfer speeds (typically 1 to 2 Mbps). In practice, Bluetooth is mainly used for peripheral sharing and short range services between PDAs, cell phones and PCs.
- IEEE 802.15.4 is a sub-standard that addresses the needs of low rate wireless personal area networks or LR-WPAN, often referred to as ZigBee. In practice, ZigBee has been utilised for automation of energy management, home and building system management (lighting, heating and cooling systems) and utility monitoring.
- The IEEE 802.11 family of standards provide specifications for high-speed networks that support most of today's wireless applications. The IEEE 802.11

specifications are wireless standards that specify an 'over-the-air' interface between a wireless user and a base station or access point (e.g. laptop to wireless access point), as well as other wireless users (e.g. a connection from one laptop directly to another laptop).

- The IEEE 802.16 standard or 'Air interface for fixed broadband wireless access systems' is commercially referred to as WiMAX. This technology is designed to provide wireless last-mile[5] broadband access in the Metropolitan Area Networks (MAN), delivering performance comparable to traditional broadband (cable, DSL, or T1) offerings. For these services, WiMAX can offer reduced implementation costs compared to wired connectivity, as there is no need for physical cabling. Potential implementations range from office wireless networks to 'whole of city' ICT enablement. Further extending WiMAX implementations, the 802.16 standard includes specification for a mobile wireless solution.

Wireless security standards

- IEEE 802.1X is a specific standard defining a framework for authenticating and controlling user traffic to a protected network, and managing and handling the various components of the framework. 802.1X supports multiple authentication methods (e.g. token cards, Kerberos, one-time passwords, certificates, and private/public key authentication).

This list of standards is in no way complete and each of the standards above is supported by extensive technical standards definition and usage guidelines. This appendix focuses on the IEEE 802.11 and 802.16 standards, stipulating the concerns, risks and vulnerabilities within this group of standards and common approaches to managing them.

Security features of wireless technologies (WiFi and WiMAX)

Both WiFi and WiMAX have been developed with a range of security features to address the need for secure wireless transmission of data. The security features listed below are those that are already integrated into the WiMAX and WiFi technologies. Configured correctly, these features enable a good foundation of wireless transmission security to be established. Additional security technologies and controls are also available to augment these features and provide for a 'defence in depth' approach, and such controls are introduced in the Threat Management section of this paper.

Security features of IEEE 802.11

The IEEE 802.11 WLAN standard has identified several services to provide a secure operating environment. Currently, these are WEP[6], WPA[7] and WPA2[8].

[5] Last-mile connectivity refers to the final connection link between carriage service providers and the recipient customers.
[6] Wired Equivalent Privacy (WEP) was the first generation of security protocol utilised to secure 802.11 wireless networks. WEP is known to have a number of exploitable weaknesses which limit its usefulness as a security protocol.
[7] Wi-Fi Protected Access (WPA) is the security protocol developed to resolve most of the weaknesses found in the earlier WEP protocol. It is based on the IEEE 802.11i standard, but does not implement all elements of that standard.
[8] Wi-Fi Protect Access version 2 (WPA2), unlike WPA, implements all of the IEEE 802.11i standard.

- **Wired equivalent privacy (WEP).** The security services for 802.11 were originally provided by the WEP protocol to protect link-level data during wireless transmission between clients and access points. WEP does not provide end-to-end security, as it only protects the wireless portion of the connection[9]. However, there are a number of widely known weaknesses in the WEP protocol and these vulnerabilities significantly limit its ability to safeguard data. Tools such as Aircrack, AirSnort, WEPCrack and dweputils are easily available for download from the Internet and have the ability to crack the WEP keys that safeguard transmissions, by analysing traffic from passive data captures[10]. For this reason, its use is not recommended unless there is no alternative.
- **Wi-Fi protected access (WPA).** An improvement on WEP is WPA which was introduced in 2003 and is based on an early draft of the 802.11i[11] specification. WPA avoids most of WEP's vulnerabilities, and increases the strength of the encryption and authentication protocols.
    - WPA can operate in one of two modes, either WPA-PSK (Pre-Shared Keys) or the standard WPA, also referred to as WPA Enterprise. WPA-PSK was developed for users who do not have access to, or the ability to utilise, an authentication server, and predominantly targets personal use. WPA Enterprise targets wireless solutions that require more robust security, such as organisational WLAN networks. WPA Enterprise requires the use of an IEEE 802.1X authentication server.
    - Wi-Fi Protected Access 2 (WPA2) is an improvement over WPA, with further strengthening of encryption capability (with options to utilise the Advanced Encryption Standard (AES[12,13])), and improved authentication and key management controls[14]. WPA2 certified devices offer the full spectrum of features outlined in the finalised 802.11i specification. A well configured WPA2 deployment offers strong wireless protection for enterprises.
    - WPA2 can be implemented in either of 2 modes, WPA2-Personal and WPA2-Enterprise[15]. WPA2-Personal is tailored towards home users and small businesses, protecting unauthorised network access using a set-up password (a pre-shared key). WPA-PSK has similar capabilities to WPA2-Personal. WPA2-Enterprise is designed for the enterprise market segment

[9] Page3-13 NIST, Special Publication 800-48, Wireless Network Security, 802.11, Bluetooth and Handheld Devices, Tom Karygiannis and Les Owens
[10] WEP Vulnerabilities—Wired Equivalent Privacy, Lee Barken, www.informit.com/articles/article.asp?p=102230&seqNum=12
[11] IEEE 802.11i is an extension to the IEEE 802.11 standard which specifies security mechanisms beyond the original WEP security included within early 802.11 standards.
[12] AES is an encryption standard which is considered suitable for protecting sensitive organisational data. See reference 13.
[13] CNSS Policy No. 15, Fact Sheet No. 1 – National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information, CNSS, June 2003, http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf
[14] Wi-Fi Protected Access 2 (WPA2) Overview, Joseph Davies, May 2005, http://technet.microsoft.com/en-us/library/bb878054.aspx
[15] WPA2 – Q&A, WiFi Alliance, www.wifialliance.com/files/kc_11_WPA2%20QandA_3-23-05.pdf

and provides for authentication of users through RADIUS[16], allowing organisations to gain leverage from investment in their existing 'wired' infrastructure.

WPA-PSK[17] is the current minimum recommended standard and WPA2 (AES) with RADIUS[18] authentication provides strong wireless protection.

Security features of IEEE 802.16

The IEEE 802.16 standard has undergone significant review by information security researchers to minimise any weaknesses in the security methods and implementation described in the specification. The current 802.16 (802.16-2005) security architecture includes the following protection methods:

- **Authentication and authorisation—**The authentication procedure is similar to WEP/WPA in that the subscriber station, such as a laptop with a WiMAX enabled access card, must first obtain authorisation from a base station prior to operation. 802.16 offers a choice from two different authentication mechanisms: RSA (a cryptographic algorithm devised by Rivest, Shamir and Adleman) and EAP (Extensible Authentication Protocol). EAP is recommended as a result of security research which highlighted weaknesses of RSA in previous 802.16 implementations.
- **Privacy and key management (PKM)**—refers to how keys are handled in a WiMAX device or during key interaction between two devices. Protecting private keys is vital for the security of a WiMAX network and its wireless data. 802.16 offers two options, PKM v1 and PKM v2. PKM v2 is recommended as a result of security research highlighting security issues in PKM v1, which were subsequently amended in PKM v2[19].
- **Data encryption**—in 802.16e-2005 can be configured to use the Data Encryption Standard (DES[20]) in Cipher-Block Chaining (CBC) mode or AES in a number of modes. The general consensus from security researchers is that AES offers better protection than DES-CBC[21] and is the recommended algorithm.

Security controls within the 802.16 standard continue to evolve. Many of the security protocol options offered in later 802.16 implementations were introduced as a result of security flaws and issues identified in earlier implementations of 802.16. It is expected that additional security issues will be uncovered by researchers as WiMAX and other implementations become more common. Security researchers have identified potential flaws in 802.16d-2004 which have not been addressed in the

[16] RADIUS is an authentication scheme (user name and password) that allows only authorised users to access the network. The system is generally considered more secure than a PSK authentication system. WPA also has RADIUS support.
[17] PSK is Pre-shared key mode (also known as *personal* mode) and is designed for home and small office networks that cannot afford the cost of more complex systems such as an 802.1X authentication server.
[18] RADIUS (Remote Authentication Dial In User Service) is an AAA (authentication, authorisation and accounting) protocol for applications such as network access or IP mobility.
[19] Security Analysis of IEEE 802.16, Maccari, Paoli, Fantacci, http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/4288670/4288671/04288868.pdf
[20] DES is an encryption algorithm which has been superseded by 3DES and AES.
[21] Ibid

current 802.16e-2005 revision, and a number of new flaws from the 802.16e-2005 standard[22,23]:

- Base station identity is not defined in the authorisation process, which may aid attackers in setting up forgery or replay attacks.
- A variety of possible denial of service attacks have been highlighted.
- The new 'mesh mode' that supports mobile devices introduces potential threats in multi-hop mesh networks.
- The mesh mode authorisation process may be susceptible to replay attacks.
- The operator shared secret (OSS) may be intercepted by attackers and leveraged to gain unauthorised access on a meshed WiMAX system.

As these issues are not currently subject to known or demonstrated exploits, existing WiMAX technologies are currently considered robust when securely configured with the controls offered by 802.16e-2005.

When considering a WiMAX deployment, adopters should ensure that the service provider's implementation offers a security service level commensurate with the orgnaisation's risk tolerance. Specific items to look for include the authentication and authorisation protocols and configurations used, and the encryption model used.

Authentication using 802.1X

In an enterprise environment, strong wireless authentication is provided by the IEEE 802.1X authentication scheme. This verifies whether a wireless device is authorised to utilise the network that it is trying to access. The following describes at a high level, how authentication in 802.1X generally occurs:

[22] Ibid
[23] Security of IEEE 802.16 in Mesh Mode, Yun Zhou and Yuguang Fang
http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4086474

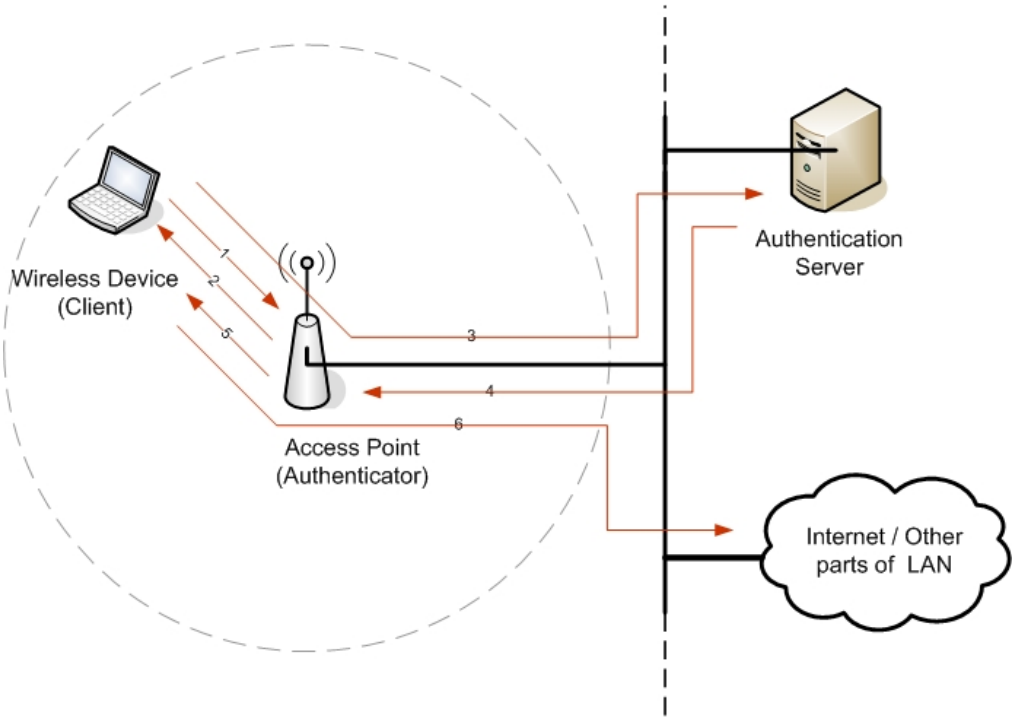


Figure 2: Authentication in 802.1X wireless environment

1) The unauthenticated client (wireless device) is within range of a broadcasting wireless access point. The wireless device sends an authentication message to the authenticator (the wireless access point) requesting access to the network.

2) The access point responds with a port address for the wireless device to communicate with. The port allows the wireless device to communicate with the authentication server—proxied via the access point—for the purpose of authentication.

3) The wireless device then sends another authentication message to the access point, which is proxied to the authentication server.

4) The authentication server receives the message, and uses an authentication algorithm (or other means depending on the way the server is configured) to assess whether the identification is valid or not.

5) The authentication server then sends a message to the access point, telling it to accept the connection (if the wireless device is valid) or reject (if the wireless device is not valid).

6) If accepted, the access point then opens up relevant LAN ports for the now authenticated wireless device.

Wireless threats

Wireless security risks

At a high level, risks can be categorised under the three main categories identified in the *TISN Wireless Security—CIO Report*. These are loss of:

- confidentiality.
- integrity.
- availability.

Discussion of the sources of some of these risks from a technical perspective is included below:

- Radio frequency is a fundamentally different medium to physical cables and has different properties that make it more difficult to secure. Failure to adequately understand these properties may lead to incorrect deployment choices that impact security.
- Misconfiguration of wireless devices can expose organisations to many security issues. Wireless products are typically designed to work out of the box and will have minimal security by default. This makes wireless networks incredibly easy to set up but also means that the majority of deployments are insecure. To further compound this problem, security options are complex and often troublesome to get working correctly.
- Many network vulnerabilities that have been analysed and controlled in wired network environments also occur in wireless networks. These threats exploit properties of the wireless medium, such as the difficulty of tracking and monitoring devices to make old attacks new again.
- As with wired networking technologies, wireless systems are susceptible to attacks based on the underlying protocols of the system. Most wireless systems utilise TCP/IP or other data communications protocols, and any attacks that can be performed using these protocols will be possible on the wireless systems.
- Wireless technologies (Wi-Fi in particular) generally have basic security mechanisms as part of their design. There have been instances where research has uncovered critical flaws in their design and/or implementation that render these security features ineffective. In the case of Wi-Fi, these basic security measures are still included as security options in wireless products. Many users who are not aware of the vulnerabilities continue to use these flawed security controls.

Attacks on wireless networks

Wireless technologies may be susceptible to both passive and active attacks. The US National Institute of Standards and Technology (NIST) define six different types of attacks under these categories for WiFi technology[24]. These attacks are applicable to

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

wireless technologies that organisations commonly use, whether fixed, mobile, short range or long range.

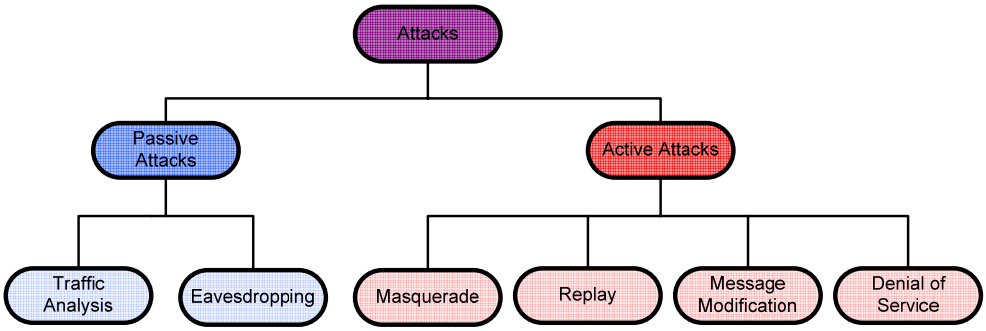


Figure 2: Taxonomy of security attacks

- **Passive attack**—An attack in which an unauthorised party gains access to an asset and does not modify its content. Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis) and are described below:
  - **Eavesdropping**—The attacker monitors transmissions for message content. An example of this attack is a person listening in to the transmissions on a LAN between two workstations or tuning into transmissions between a wireless handset and a base station.
  - **Traffic analysis—**The attacker 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 unauthorised party makes modifications to a message, data stream or file. It is possible for these attacks to be detected but they may not always be preventable. Active attacks may take the form of one of four types (or combination thereof):
  - **Masquerading**—The attacker impersonates an authorised user and thereby gains certain unauthorised 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.

Sample attacks for WiFi networks

The following is a list of sample security attacks for disclosed wireless vulnerabilities. This list is included to raise awareness of attacks that occur, and is not a complete or exhaustive list of possible attacks/exploits.

- **Exploitation of software/firmware vulnerabilities in wireless networks/devices**

- Multiple instances have occurred of mainstream wireless access points or routers having ‘backdoor’ logins (e.g. Login: super, Password: super).
- Wi-Fi driver attacks which allow attackers to gain access to ‘root’ privileges.

- **Denial of service attacks**
  - Overwhelming nodes with excessive traffic.
  - Exploitation of flaws in the network protocol implementations offered by the wireless device.
  - Disassociating wireless clients to continually disconnect from networks.
- **Cracking authentication protocols**
  - Some wireless login protocols are vulnerable to dictionary attacks and precomputation attacks, where malicious users passively collect wireless data exchanges, then use the packets to determine keys.
- **‘Evil Twin’ attack**
  - The installation of an extra wireless access point posing as a legitimate organisation-owned access point. If legitimate clients attempt to associate with the rogue access point, the malicious user could steal or capture any authentication credentials utilised.

The security management techniques and practices identified in the threat management section of this technical appendix will reduce the likelihood or impact of attacks on wireless systems and help manage the organisation’s risk exposure.

Security tools for wireless networks

There are a number of security tools for testing and compromising wireless security configurations. More common tools for WiFi security include the following:

- **Kismet**—wireless network detector, sniffer and intrusion detection system
- **NetStumbler**—Windows based wireless network detector and sniffer.
- **Aircrack**—A tool that can break WEP and WPA encryption keys.
- **Airsnort**—A tool that can break WEP and WPA encryption keys.
- **KisMAC**—Mac OS based wireless network detector and sniffer.
- **Aireplay**—Part of the aircrack suite, this tool is used for wireless packet replaying.

Currently there are limited WiMAX security tools available for testing or compromising deployments. Tools include the following:

- **Wireshark**—includes the ability to read WiMAX captures.
- Specific commercial products.

Common tools for testing or compromising Bluetooth security include the following:

- **Bluediving**—Bluetooth penetration testing suite.
- **Bluescanner**—Bluetooth device scanner.

- **BTCrawler**—Bluetooth diagnostic tool.
- **CIHWB**—Bluetooth security auditing tool for Windows Mobile 2005.

Threat management

Security countermeasures for wireless networks

The US NIST has suggested countermeasures at the management, technical and operational level for securing wireless networks. These include:[25]

Management countermeasures

Management countermeasures for securing wireless networks begin with a comprehensive security policy. A security policy, and compliance therewith, is the foundation on which other countermeasures—operational and technical—are rationalised and implemented. Wireless security policies should include the following items:

- **Authority and responsibilities of users**—The policy should outline what is covered by the policy, why the policy is necessary and what can happen if the policy is breached. It should also define the responsibilities of departments and individuals, particularly general users, IT departments and auditors.
- **Assets to be protected**—The policy should identify or make reference to the sensitive information assets, communications channels and systems that wireless security will be protecting.
- **Threats and vulnerabilities**—The policy should include a section which identifies the threats to organisational wireless systems.
- **Impact analysis**—The policy should identify the consequences of a wireless security breach.
- **Procedures and responses**—The policy should identify and define security procedures for the following items:
    - User account creation.
    - Password policy and resets.
    - Authentication.
    - Site and equipment access.
    - Security breach reporting.
    - Disposal of sensitive data.

- **Incident response planning**—should be described including response plans for various incidents, authority and responsibility, investigation processes, remediation planning and what reporting needs to take place.
- **Acceptable usage**—Policies should be created that identify the activities for which wireless resources are authorised for use (e.g. internet access, email and

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

job duties). The policy should also identify activities that are specifically prohibited, with explanation of the need to protect corporate assets and to maintain the integrity of networks and systems.

- **Endpoint security**—Controls for securing workstations, laptops, PDAs and other wireless devices should be included in wireless policies. Requirements for frequent/up-to-date patching, mandated use of security software as appropriate (e.g. VPN clients, anti-virus, and personal firewalls), should be included. The controls listed may have to account for different access situations, particularly when accessing organisational resources on-site or off-site.
- **Deployment guidelines**—Policies should provide guidelines for the implementation and deployment of wireless systems and architectures. The policy should describe who can install access points and other wireless equipment, and provide limitations on the location of and physical security for access points. It should also supply default configurations for both access points (utilise WPA2 / 802.11i) and endpoint devices (utilise a VPN), authentication (utilise 802.1X based authentication) and confidentiality mechanisms, key management requirements, and physical and network placement requirements.
- **Deployment policies**—should also account for the change management of deployed infrastructure, such as device registration, procedures for device upgrades, removals and additions, as well as configuration and interoperability testing.
- **Auditing and compliance**—The policy should include requirements for audit logging and accounting, including which actions and events to log, and frequency of log review. Policies should also define the frequency and scope of security assessments to include access point discovery.
- **Policy enforcement**—The policy should outline the monitoring responsibilities of staff, and an escalation process should be established for any breaches that are to be raised. The policy should detail disciplinary action for breaches/repeated breaches.
- **Regulatory obligations**—Wireless policies must consider any relevant industry standards (e.g. Payment Card Industry Data Security Standard (PCI-DSS)) or guidelines for data privacy and protection.
- **Training and awareness**—Along with a robust security policy framework, organisations 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 wireless networks and devices pose. They must work to ensure security policy compliance and to know what steps to take in the event of an attack. All wireless users should also be made aware of their responsibilities when utilising corporate wireless networks or connecting mobile computing devices to any wireless network outside the organisation.

Operational countermeasures

Physical security is a fundamental step for ensuring that only authorised users have access to wireless computer equipment. As with facilities housing wired networks, facilities supporting wireless networks need physical access controls. Physical security combines measures such as:

- access controls—photo identification, card badge readers, or biometric devices can be used to minimise the risk of improper penetration of facilities
- personnel identification
- external boundary protection—locking doors and installing video cameras for surveillance around the perimeter of a site to discourage unauthorised access to wireless networking components, such as wireless access points (APs).

While such steps are important, in a wireless environment an attacker or intruder can be located outside your physical perimeter but still be within the proximity of your wireless network and consequently be able to enter the network. To address this, organisations should use wireless security assessment tools (e.g. vulnerability assessment) and regularly conduct scheduled security audits. Security audits are conducted to assure the compliance of devices and employees to organisation policy. Penetration testing can also occur to ensure the wireless system risks continue to be within the risk tolerance of the organisation.

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) configuration, 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), network segregation and biometrics. It should be noted that some of these solutions are now available either in hardware or software.

Technical countermeasures should also include facilitation of encryption and authentication controls described in each wireless standard. Encryption in wireless communication is used primarily to protect the confidentiality of messages and connection setup data transmitted over the network. Authentication in wireless networks occurs to validate connections between one device and another, or to confirm that a user is permitted to connect to a particular network.

- Encryption protocols utilised in past wireless standards have been found to be insecurely implemented and consequently easy to defeat (e.g. WEP RC4). Utilising the most current revisions of wireless standards is recommended, as they tend to allow use of highly secure encryption protocols that have yet to be defeated (e.g. WPA2's AES protocol). The actual choice of encryption protocol utilised is dependent on organisational infrastructure:
    - Legacy devices may only support WEP/TKIP, and not support WPA/WPA2.
    - AES requires greater processing power.
    - Best practice encryption for WiFi connections is currently WPA2 utilising AES.
- Many wireless technologies allow a number of authentication modes to be used, which offer differing authentication strengths. For example, WPA and WPA2 can be figured in Personal or Enterprise mode. Personal mode utilises the weaker PSK authentication, and Enterprise mode requires the much more robust 802.1x/EAP authentication method. Depending on the business use cases, either authentication mode may be more suitable.

- For large networks that require a more manageable solution, the centralised authentication and management utilised by 802.1x with an appropriate EAP choice is recommended.
- For small or temporary networks, a pre-shared key may provide adequate protection.
- Best practice authentication for WiFi connections is currently via WPA2 using 802.1x/EAP.

- It should be noted that legacy systems or devices may not be compatible with the most current standards, and additional infrastructure (e.g. an authentication server) may also be required to successfully implement security protocols.
- It is good security practice to disable the network service set identifier (SSID[26]) from broadcasting on WiFi infrastructure. This prevents the access point from announcing its presence.

Additional security measures can be utilised beyond the included security functionality of wireless standards and their associated technologies. In many cases, these additions can greatly increase the protection levels offered to organisational data when using wireless networks. Additional measures include:

- Utilising a virtual private network (VPN) to add an additional layer of security for remote access. When utilising a wireless network or hotspot that does not belong to the organisation (e.g. home or community WLANs), use of a VPN is highly recommended. The additional layer provides stronger authentication and encryption for the remote access user.
- Wireless intrusion detection systems (IDS) are a technology utilised to detect wireless specific attacks. Utilising a Wireless IDS can allow an organisation to react to security attacks as early as possible and minimise any impacts. A wireless IDS can further be utilised to enforce policy and trigger management operations, such as locking down or deauthenticating a suspicious user, or switching wireless channels to improve signal strength.
- Hard disk/storage encryption is also highly recommended for sensitive organisational information stored on any wireless enabled devices due to the general portability that accompanies such devices.

[26] SSID is an identifier for a wireless LAN. These can be broadcast by the wireless access points that belong to the network.

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.

www.wi-fi.org/

This is the website for the Wi-Fi Alliance, a group which certifies and ratifies Wi-Fi IEEE 802.11 implementations. It provides information on Wi-Fi devices and includes a directory of articles and responses on various aspects of both Wi-Fi and Wi-Fi security.

www.wimaxforum.org/home/

This is the website for the WiMAX Forum, a group which certifies and ratifies WiMAX IEEE 802.16 implementations. It provides information on WiMAX technology and updates, business cases and regulatory information.

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.

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.

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.