mwr InfoSecurity

WiFi: White Paper

Key Principles

- An AP (Access Point) is a radio transmitter and receiver.
- Radio waves travel outwards from a broadcast point in a similar manner to light travelling outwards in all directions from a star.
- Large physical objects interfere with or absorb radio signals.
- Weaker signals have a decreased radius of travel.
- A directionally controlled signal can have its broadcast area controlled.
- Radio waves travel on different frequencies, such as 2.4ghz.
- If there are 2 AP's broadcasting on the same channel there is a chance that they will compete, cancel each other out and become unusable.
- For anyone to identify a broadcasting system all they need is to be within range of an AP signal and have a transmitter / receiver (PC wireless card).
- Access can be controlled to a certain degree using various methods. Using default configurations / nothing / one method is simply not secure.
- WEP keys are not 100% secure.
  (The first 24 bits of the data frame that activates WEP are in plaintext and not encrypted; once this is captured it is possible to break the encryption).

WiFi Standards

802.11 WiFi (Wireless Fidelity) standards are produced by the Institute of Electrical and Electronics Engineers (IEEE), a non-profit, technical professional association.

The 802.11 standard is now in its seventh version, g (a more secure Advanced Encryption Solution 802.11i is on the horizon). It is the fourth WiFi product certification from the IEEE and is available for download at http://standards.ieee.org/getieee802/download/802.11g-2003.pdf

802.11g Overview

Previous IEEE certification programs were for products based on the 802.11a and 802.b standards, including dual-band products as well as the IEEE's own 'WiFi Protected Access'.

802.11g lays out the ground rules for Wireless LAN equipment that is capable of at least 24Mbps (megabits per second) and up to 54Mbps, while remaining backward compatible with existing 802.11b equipment that runs at a maximum 11Mbps. Both use radio spectrum in the 2.4GHz radio band. Another standard, 802.11a, defines 54Mbps gear in the 5GHz range.

Certification means that products are compatible with one another.

The growing number of amendments to IEEE's family of 802.11 wireless Internet standards and vendors' use of different chip sets within the same product line have created a need for interoperability testing and certification.

The key issue with 802.11 standards is that they are mainly focussed on the functionality of WiFi equipment. There is little specific detail regarding the securing of WiFi equipment in a networked environment.

802.11g is frequently referred to in relation to network security. It is relevant in terms of interoperability but that is the only part it can play in a security discussion. It is only when a system (group of devices) is fully functional that the security problem can be tackled.

In short 802.11g enables security rather than ensuring it.

mwr InfoSecurity
1st floor . Brook House . Alençon Link
Basingstoke . Hants . RG21 7RD . UK
+44 (0)1256 300920
www.mwrinfosecurity.com
info@mwrinfosecurity.com

WiFi: White Paper

Test Tools

Tools are freely available that crack the keys used to secure wireless networks and explore and enumerate the systems they protect. In testing mwr InfoSecurity uses the following tools:

- Kismet: Linux based 802.11 layer2 wireless network detector, sniffer, and intrusion detection system.
- NetStumbler: Windows utility for 802.11b based wireless network auditing.
- GpsDrive: used to map AP positions based on received NMEA GPS data.
- WEPCrack: breaks secret 802.11 WEP keys
- AirSnort: WLAN tool that recovers encryption keys. AirSnort operates by passively monitoring transmissions and computing the encryption key when enough packets have been gathered.
- Nmap: utility for network exploration or security auditing.
- Ethereal: packet capture and analysis.
- Ettercap: multipurpose sniffer/interceptor/logger for switched LAN's.

Testing Methodologies

mwr InfoSecurity only ever conduct tests that follow an organised and proven methodology.

This ensures consistency, absence of false-positives and credible results.
Our wireless testing service adheres to the following methodologies:

Access Point Verification
Access points (AP's) allow clients to connect to the wireless network. AP's may be attached to part of an internal wired network. AP's come with default configurations. Default configurations are frequently maintained post implementation. The nature of default configurations is that they are inherently insecure - such settings offer low security. AP's are often left open to the public domain.

This methodology attempts to identify and distinguish all client AP's and their configuration.

Gather and Analyse Packet Data
As part of the AP verification method packet data is captured and stored for analysis. This method is used to identify all data, encrypted or otherwise. Unencrypted data gives open view of network traffic. Encrypted data packets are captured and stored for later use in cracking WEP encryption.

DoS Testing
AP's can be vulnerable to Denial of Service (DoS) attacks. Using packet crafting tools and techniques (such as Ettercap) AP's will be tested for known DoS attacks.

WEP Key Cracking
Due to the flawed methods used in WEP encryption there are opportunities to crack it. Tools are available which take advantage of weak Initialisation Vectors used in both 40bit and 104bit WEP encryption. With enough captured encrypted packets it is possible to break WEP encryption in a short amount of time.

WiFi: White Paper

Best Practice

Due to the current state of wireless technology a totally secure wireless network is an ideal rather than a practical possibility. Many vendors provide inadequate product information regarding the fundamental principles of WiFi, and therefore give users little opportunity to protect their AP’s from abuse.

The following best practice recommendations should become part of any organisations information security policy. They will ensure that your wireless network is as secure as currently possible.

- **SSID**
  Disable Broadcast SSID: Change to a non-descriptive SSID

Change the default SSID’s for your AP. Never use obvious SSID’s such as addresses, company names or locations.

Where possible use a set up that allows you to disable SSID broadcasting (known as "closed system" or "disable broadcast SSID"). Like WEP and passwords this is by no means robust, but it adds a layer of security.

- **MAC Address**
  Filter by MAC address

MAC address filtering creates an environment where only permitted wireless hardware can communicate with your AP. This is an access rather than a security issue but it serves both purposes well.

This method should never be used as the sole source of access control - it is possible to create spoofed MAC addresses that bypass the ACL. As with SSID this is by no means robust, but it adds a layer of security.

- **Vendor**
  Change vendor specific default configuration: Change default AP password(s)

An intelligent Internet search will allow you to gather most default vendor AP configurations- these are commonly used by attackers to compromise AP’s. As with SSID’s, change default passwords as most products have weak out-of-the-box password settings.

AP’s are no different. Passwords must be changed before any other configuration takes place, as in their absence the AP is wide open to attack.

- **Channel**
  Change default channel configuration: Configure multiple AP’s so that there is an optimum difference of 5 channels between each AP

If you have multiple AP’s be aware of the potential for your set up to produce its own Denial of Service (DoS).

Too many AP’s trying to operate or broadcast their data using the same channel in close proximity may cause a disruption to their signals. The result is that the AP’s compete and subsequently fail to function. Where possible configure a 5 channel difference between AP’s to minimise this possibility.

WiFi: White Paper

BEST PRACTICE (CONTINUED)

- **WEP**
  Enable 128 (‘104’) bit WEP

As a low level deterrent enable the AP’s WEP security. WEP attempts to secure access to your wireless network and also encrypts data transmitted. It is possible to break but it does increase the work needed to gain access. Make sure you use the largest WEP key size that your equipment supports.

- **Broadcast Area**
  Control your broadcast area: Wave point placement and antenna selection

Increasingly available are wireless AP’s and antennas that allow you to adjust signal strength and direction. To decrease signal leakage (unrestrained AP broadcast) AP’s should be as far away from walls and windows as is practicably possible. Signal strength should be adjusted so that connection becomes difficult when near those walls. The signal should be set to point toward the centre of the building if you are using a directional set-up.

In all cases reflectors should be used as much as possible to attempt to contain the wireless data. This decreases leakage but does not eradicate it.

- **Users**
  Authenticate: Limit access rights and addresses: Use RADIUS (Remote Authentication Dial-In User Service)

Treat your wireless network as you would a VPN. Firewall all wireless networks from wired networks and ensure users log in as if accessing a wired network remotely. This separates users of wireless networks from wired networks and allows administration staff to control and log access to different parts of the network.

There are occasional instances where every user might need wireless access. Typically most users require only wired access to the network. Provide access to wireless networks only when absolutely necessary. This should be determined solely by the needs of the business and implemented in accordance with a wireless policy. AP’s should be set to only allow access to wireless cards with authorised MAC addresses.

Where wireless users make up a small percentage of total users you could use the DHCP (Dynamic Host Control Protocol) to assign a set number of addresses (corresponding to the number of users you have). If an authorised user cannot logon it indicates that there are unauthorised logons and that the AP is being abused.

RADIUS is a fairly simple protocol used to authenticate remote access. The server that implements it is often called a ‘triple A’ server (Authentication, Authorisation, Accounting). RADIUS servers negotiate access for DSL, VPN, mobile cellular and WLAN users. RADIUS servers provide another authentication layer. They are available in both commercial and open source versions and can be easily be implemented in many wireless networks.