

# Detecting and Investigating Wireless LAN Security Breaches

Leon Stringer

leon.stringer@ntlworld.com

## ABSTRACT

The rapid growth in wireless networking technologies has taken place against a backdrop of inherent security issues and new types of attack. Poor understanding of these issues combined with the ability of attackers to operate wirelessly from a distance presents many challenges for the investigator attempting to detect, verify and gather evidence of such attacks. This paper analyses the security issues and possible attacks, and examines how they may be investigated.

## Categories and Subject Descriptors

C.2.0 [Computer Systems Organization] General --- Security and Protection; K.5.0 [Computing Milieux] Legal Aspects of Computing --- General

## General Terms

Security, Human Factors

## Keywords

Cracking, hacking, wireless, WLAN, Wi-Fi, IEEE 802.11, forensic

## 1. INTRODUCTION

Wireless LANs (WLANs) have seen widespread adoption since they were first introduced around five years ago and can now be found in the home, offices, cafés and bars, and general access hotspots are available in civic spaces in some areas.

However, WLAN systems come with a host of security issues primarily the fact that network traffic is being broadcast “over the air” and can be received by anyone with suitable equipment, and the possibility of wireless access being used as a gateway to your network. Despite this, security concerns often give way to other demands notably the desire for rapid deployment.

This paper will give a brief background on the technology and issues relevant to the discussion, and then analyse the type of security breaches that may be encountered along with how they may be detected and analysed. Finally, some example prosecutions are listed by way of illustration.

This is an unpublished essay written as part of an MSc course in Computer Science.

December 8, 2005

## 2. WIRELESS LAN TECHNOLOGIES

Since the security issues surrounding WLAN systems exploit the physical or technological aspects, it is important to have an understanding of how WLANs work. The prevalent standards for WLAN systems are those branded under the umbrella term “Wi-Fi” which this paper will concentrate on.

### 2.1 Wi-Fi

The trademarked term Wi-Fi (“Wireless Fidelity”) covers a set of IEEE 802.11 standards, currently IEEE 802.11a, 802.11b and 802.11g, and is overseen by the non-profit industry body the Wi-Fi Alliance [17] who certify product interoperability; certified products may be labelled as such.

#### 2.1.1 Wi-Fi components

The main components of a Wi-Fi LAN are [3]:

- Access points (APs): Stations providing access to services via the wireless medium for associated stations.
- Stations: Fixed or mobile devices that use wireless network communication (e.g. laptops, printers).
- Wireless Medium: The medium via which data is transferred between peers on a wireless local area network.

#### 2.1.2 Wi-Fi architecture

Wi-Fi LANs have two architectural modes:

1. Infrastructure: wireless stations communicate with each other and other network resources via an AP.
2. Ad hoc: wireless stations communicate directly with each other.

Although not specifically identified in the 802.11 standards, another common set up is to combine two APs to bridge a LAN wirelessly, e.g. between two neighbouring sites.

## 2.2 Use of the “wireless medium”

Communication via the wireless medium is via transmission and reception of radio waves, using an unlicensed part of the spectrum (2.4GHz) with the standards specifying modulation techniques, channels and power output. Countries may have legal regulations governing radiocommunications usage and in some areas these overlap with Wi-Fi outlawing certain usage in some areas (e.g. prohibiting the use of some channels).

### 2.2.1 Channels

The Wi-Fi standards specify channels – fixed frequency ranges – for use with WLANs. Intercommunicating Wi-Fi equipment must be set to use the same channel. Neighbouring APs must be configured to use different channels to prevent interference. Channel selection has also been reported to have some bearing

on signal propagation relating to coverage.

### 2.2.2 Antennas

Signal transmission and reception is of course via an antenna. Many interface cards for stations and access points have a built-in antenna although for improved coverage, an external antenna can be used. There are three types of antenna in use:

1. Omni-directional: Transmission radiates out equally in all directions (in the plane of the antenna).
2. Sectorised (also known as a patch or panel antenna): Transmission radiates out in an arc.
3. Directional (also known as beam): Transmission radiates out in a tight beam.

The standard (and statutory) limits on transmitted power limit Wi-Fi's range to around 50-100m. Often the range is less due to environmental factors leading to signal attenuation, such as building materials used or local interference (by other legitimate users of this part of the spectrum).

## 2.3 Security features

The IEEE 802.11b standard includes the following security features [4]:

1. Service Set Identifier (SSID): The SSID is used to identify the AP to WLAN devices. If the AP is configured not to advertise this name, clients are required to know the SSID before connecting.
2. MAC address filters: The AP can be configured only to allow connections from a configured list of known MAC addresses.
3. Encryption: The IEEE 802.11 standard included the WEP (Wired Equivalent Privacy) encryption system intended to give wireless network traffic the confidentiality of a wired LAN.

### 2.3.1 WEP's deficiencies

After publication of the standard and widespread adoption of 802.11b equipment, WEP (Wired Equivalent Privacy) was found not to provide what its name suggested; the most notable study into its flaws by Borisov *et al.* found that "...WEP contains several major security flaws [that] give rise to a number of attacks, both passive and active, that allow eavesdropping on, and tampering with, wireless transmissions" [5]. The flawed implementation of WEP led to a fundamental redesign of the encryption mechanism in the form of WPA (Wi-Fi Protected Access). WPA is an early implementation of two security features of IEEE 802.11i:

1. 802.1X authentication: Users must supply an individually assigned password to access the WLAN.
2. Temporal Key Integrity Protocol (TKIP): Encryption keys vary as they are dynamically renegotiated between the AP and the station.

Implementation of the final IEEE 802.11i standard is known as WPA2. For optimum security, Wi-Fi operators must use an IEEE 802.1X-compliant security back-end. Although WPA was designed to be able to work on any existing Wi-Fi system via a software upgrade, there are still many WEP-only devices in use until manufacturers issue updates (if at all) and administrators deploy them.

Some manufacturers offer additional proprietary security features in their Wi-Fi products.

## 2.4 Security issues

The key security issue is that network traffic is being broadcast through the wireless medium [2]:

"Traditional wired networks use cables to transfer information, which are protected by the buildings that enclose them. To access a wired network, a hacker must bypass the physical security of the building or breach the firewall. On the other hand, wireless networks use the air, which is an uncontrolled medium. Wireless LAN signals can travel through the walls, ceilings, and windows of buildings up to thousands of feet outside of the building walls. Additionally, since the WLAN medium is airwaves, it is a shared medium that allows any one in proximity to 'sniff' the traffic."

There is a less well-defined security issue which we will term "reckless deployment", grouping situations where the security issues have not been properly considered and factored into the implementation. This may occur in cases such as:

- Unrealistic deployment timescales lead to compromised security;
- Those responsible for deployment are not versed in WLAN technology and the security implications.

Indeed when time is tight, security can often be seen as a burden, a serious mistake as it exposes an organisation to potentially avoidable threats and potential liability. Flawed as some of the early security mechanisms are they at least go some way to mitigating the risk of a security breach.

## 3. SECURITY THREATS

The new use of technology in Wi-Fi gives rise to some new breeds of attack. But such is the nature of Wi-Fi networks, particularly those with poorly deployed security, not all threats are attacks.

### 3.1 Types of attack

#### 3.1.1 Passive attacks

Traffic analysis would be a typical mechanism for examining any security mechanisms with a view to defeating them. For example, continued monitoring may allow decryption through brute force attacks or at least allow enough knowledge to be gained to mount an attack through replay. Unencrypted or decrypted traffic could be used to gain knowledge of network structure, user passwords or confidential information. It also allows the discovery of valid MAC addresses; setting unauthorised equipment to use these is trivial.

#### 3.1.2 Denial-of-service

Wenyuan, et al. describe four types of jamming-style denial of service attacks [16]:

1. Constant jamming: A continuous signal either generated by Wi-Fi equipment not conforming to protocols (e.g. through software modification) or generated by some form of waveform generator.
2. Deceptive jamming: Transmission of apparently legitimate packets with no gap that keeps normal users in the receive state and consequently unable to transmit.
3. Random jamming: Switching between silence and constant or deceptive jamming, perhaps to conserve power or evade detection.
4. Reactive jamming: Remaining silent while the channel is idle and again employing one of the first two techniques when activity is detected.

### 3.1.3 Replay

A replay attack would follow a period of passive listening to traffic and then transmitting previously recorded traffic which would appear legitimate but would have undesired effects. Note that it is not necessary for the recorded traffic to have been understood, it may be the retransmission of encrypted traffic to examine responses and study security mechanisms.

### 3.1.4 Message modification

Similar to a replay attack this would involve modifying part of the recorded message before transmission. Again, the modification may not be understood by the attacker who may perform many iterative modifications looking for clues that could be used to defeat the security.

### 3.1.5 Masquerade

This involves the attacker configuring equipment to appear legitimate to the WLAN system perhaps following some combination of the above attacks to deceive security mechanisms. This could take the form of a computer configured to gain access to the network via an AP or a bogus AP configuration for legitimate user equipment to inadvertently associate with. This is also known as a man-in-the-middle attack and may be used to obtain passwords or other details from unsuspecting users.

## 3.2 Other security issues

These issues are not necessarily attacks but concern security nevertheless.

### 3.2.1 Rogue access points

A rogue AP can be defined as “...any Wi-Fi access point connected to your network without authorization. It is not under the management of your network administrators and does not necessarily conform to your network security policies” [13]. A rogue AP is therefore a potentially unsecured gateway onto your network open to both accidental and criminal use. This can even be a problem for organisations without a WLAN installation: a rogue AP may be installed by an employee for personal use without understanding the security implications.

### 3.2.2 Accidental association

Accidental association takes place when a client device configured to automatically associate with available Wi-Fi networks, establishes a connection via an access point for a network they are not authorised to use, e.g. a neighbouring AP. If the expected network resources (e.g. Internet connectivity) are available the user may not be aware that this has happened.

### 3.2.3 Wardriving

Wardriving may be considered a special case of a passive attack where potential attackers roam an area, typically by car, with equipment used to detect Wi-Fi signals. Wardrivers then note discovered APs for later use. It is not clear whether wardriving is in itself criminal, certainly the act of merely detecting signals is not a security issue, however information gained while wardriving may lead to a later attack.

### 3.2.4 Warchalking

There is also a widely reported but less observed phenomena of warchalking where those discovering Wi-Fi coverage chalked marks to indicate this. This is generally considered to be so small scale as to not be an issue.

## 4. DETECTING AND INVESTIGATING THREATS

Passive attacks will leave no evidence on the network as it has not been interfered with. You may only become aware of this if it leads to an active attack or the information is exploited in some other way such as leaked corporate information. Passive attacks may be conducted from a safe distance; it is possible to use high gain receivers to monitor traffic from beyond the usual limits of Wi-Fi coverage. The presence of someone in the area with a laptop and antenna directed at your building may lead you to suspect a passive attack. If they are in a car, record the date, time and license plate in a log of such activity.

Masquerade attacks can also be difficult to spot since the network traffic will look like it originates from a legitimate source. An attacker careful to avoid any suspicious network activity may remain undetected. Logging and reporting on network activity may show unexpected usage that raises suspicions. Also, the legitimate user or legitimate equipment being masqueraded may experience connectivity problems indicating a possible attack.

Replay and message modification may cause unexpected network problems; again traffic logging may allow detection.

A successful denial-of-service attack should be relatively easy to detect in that the subject of the attack (e.g. an AP) will stop working. More difficult to detect would be a partially successful attack or intermittent jamming attack which might result in reduced coverage or performance which would be hard to distinguish from:

- A busy AP
- Environmental factors attenuating signal
- Legitimate interference
- A faulty AP

Once you establish such an attack, the use of monitoring tools (see next section) may help identify the source.

It is possible to “jam” from outside the normal Wi-Fi range by simply using a higher power signal. However, this may also subject the attacker to laws governing spectrum usage, and agencies with responsibilities in this area (e.g. OFCOM in the UK, the FCC in the US) may also seek to prosecute the attacker and may assist in any investigation.

Rogue APs may be identified by mapping the premises with some form of monitoring tool.

Accidental association would only happen with an unprotected AP. As this is “accidental” the advantage is that there should be relatively few impediments to investigation e.g. MAC addresses would be “real” so should be spotted with traffic analysis. It would be unrealistic (not to mention extremely harsh) to attempt to prosecute an accidental user, particularly since it would be hard to prove any intent. It would be much wiser to reappraise security and consider any liability for potentially illicit systems use and data protection.

Part of the deployment of WLANs should be a procedures and policies document. This should be a “living document” that takes awareness of the security systems in place, identifies an auditing and monitoring regime, describes how suspected issues are dealt with and allows for the security systems to be refined in light of this.

## 5. FORENSIC TOOLS

Specialist tools are becoming available which may assist the investigator.

## 5.1 Wireless intrusion detection systems

Wireless intrusion detection systems (WIDS) which extend the traditional (wired) network intrusion detection system into the realm of the WLAN are becoming available. Implementations vary but typically a WIDS will monitor wired and wireless traffic for analysis and reporting, and can be configured to deactivate APs on criteria which may indicate an attack.

AirDefense is a company specialising in the security of wireless systems and offer a range of proprietary products from those designed to run on a single computer to a suite for enterprise-wide monitoring [1]. The enterprise-level products include reporting tools aimed at those with forensic requirements.

## 5.2 Wi-Fi Detectors

Wi-Fi detectors - such as the TRENDnet TEW-T1 [15] - are hand-held devices which can be used to survey an area for use of the Wi-Fi band and can indicate this in terms of signal strength and also indicate non-Wi-Fi transmissions that may cause interference.

## 5.3 Kismet

Kismet is an "802.11 layer 2 wireless network detector, sniffer, and intrusion detection system" [9] popular with those on both sides of the security fence and includes the following potential applications:

- Site surveys: measuring and plotting coverage of Wi-Fi hotspot
- WIDS: monitoring multiple sniffers via a single server
- Rogue AP detection: locating unauthorised APs

It is free, open source software available for GNU/Linux.

## 6. ATTEMPTED PROSECUTIONS

### 6.1 Case 1

In 2004, three men were convicted using unsecured APs installed at branches of Lowe's home improvement store to access customer credit card information. During a wardrive, unsecured access was discovered at a Lowe's branch in Michigan. They used this access to route to stores in several states. Reportedly, Lowe's network engineers noticed unusual transactions, began monitoring activity and contacted the FBI. They traced the activity to the Michigan store and the three were arrested after being observed parked in the store car park with antennas and a laptop.

The three received custodial sentences [6, 12].

### 6.2 Case 2

In 2005, a man was convicted under the Communications Act (2003) for the use of domestic APs, in London, UK. He was arrested following complaints from residents and was caught in a residential area with a wireless-enabled laptop.

He was fined £500 and given a 12-month conditional discharge [8, 10].

### 6.3 Case 3

In 2004, a man was convicted of using unprotected APs to send adult-themed spam in California. He had been wardriving looking for unsecured APs in residential areas which were then used for the transmission of the email [7, 11].

## 6.4 Case 5

In 2003, a man was arrested in Toronto, Canada after being discovered by police naked from the waist down sitting in his car while downloading child pornography via an unsecured AP [14].

This case raised the issue of the possible liability of the unsecured AP owner.

## 7. CONCLUSION

The momentum behind WLAN adoption shows now sign of abating and the security mechanisms available belatedly becoming suitable for mainstream use. However, failure to leverage this security whether for reasons of time, compatibility or ignorance means WLANs will persist as a fairly soft target for the foreseeable future. Even with good security in place, the threat is only reduced, not removed. The public nature of the wireless medium allows the tenacious attacker to conduct their campaign at a discrete distance over an extended period.

Despite the difficulties, it is possible to secure a conviction for criminal WLAN use. However, it is surely only a matter of time before a WLAN operator faces prosecution for failing to implement suitably rigorous security leading to some form of liability either through crimes committed via their network or failing to secure information held on their network.

The particular difficulties in investigating such cases can be summarised as follows:

- Wireless access: attackers and other sources of problems are physically removed from the network;
- The ability for an unauthorised user to access network resources in a manner that is difficult to distinguish from an authorised user;
- The ability of an attacker to monitor network traffic remotely with absolutely no indication that this is taking place.

These issues are often compounded further by poor management of WLANs and an organisation looking to facilitate any investigation should:

- Analyse and implement suitable security mechanisms for the environment;
- Tie these into procedural documentation such that the two improve as issues arise;
- Implement some form of traffic logging;
- Implement some form of WIDS;
- Maintain lists of APs along with their location and coverage;
- Maintain lists of MAC addresses in use in the organisation;
- Periodically survey the immediate locale for illicit or unauthorised activity (e.g. rogue APs).

An investigator looking to specialise in this area would need:

- A good working knowledge of WLAN technologies;
- An understanding of the kind of attacks specific to WLANs;
- Practical knowledge of the tools available;
- An understanding of the legal and regulatory framework for any potential prosecution.

There is no doubt that the requirements for these skills will become increasingly important in the future.

## 8. REFERENCES

- [1] Air Defense  
<http://www.airdefense.net/>
- [2] Air Defense Whitepaper: Wireless LAN Security: What Hackers Know That You Don't  
<http://www.airdefense.net/whitepapers/>
- [3] ANSI/IEEE Std 802.11, 1999 Edition (R2003)  
<http://standards.ieee.org/getieee802/download/802.11-1999.pdf>
- [4] Bhagyavati, Summers, W.C. and DeJoie, A. Wireless Security Techniques: An Overview. In *Proceedings of the 1st annual conference on Information security* (Kennesaw, Georgia 2004). ACM Press, New York, NY, 2004, 82 – 87.
- [5] Borisov, N., Goldberg, I., Wagner, D. Intercepting Mobile Communications: The Insecurity of 802.11. In *Proceedings of the 7th annual international conference on Mobile computing and networking* (Rome, Italy). ACM Press, New York, NY, 2001, 180 – 189.
- [6] Dept. of Justice press release: Three Plead Guilty to Computer Hacking  
<http://charlotte.fbi.gov/dojpressrel/2004/lowescomputerhack.htm>
- [7] Dept. of Justice press release: Guilty plea by local 'war-spammer' is first-ever conviction under CAN-SPAM act  
<http://www.usdoj.gov/usao/cac/pr2004/131.html>
- [8] Ilett, D. Wireless network hijacker found guilty  
<http://management.silicon.com/government/0,39024677,39150672,00.htm>
- [9] Kismet  
<http://www.kismetwireless.net/>
- [10] Leyden, J. UK war driver fined £500  
[http://www.theregister.co.uk/2005/07/25/uk\\_war\\_driver\\_fined/](http://www.theregister.co.uk/2005/07/25/uk_war_driver_fined/)
- [11] Poulson, K. Plea deal in 'war spamming' prosecution  
[http://www.theregister.co.uk/2004/09/04/war\\_spamming\\_plea/](http://www.theregister.co.uk/2004/09/04/war_spamming_plea/)
- [12] Poulson, K. US wardriver pleads guilty to Wi-Fi hacks  
[http://www.theregister.co.uk/2004/06/07/us\\_wardriver\\_guilty\\_plea/](http://www.theregister.co.uk/2004/06/07/us_wardriver_guilty_plea/)
- [13] Proxim White Paper: Rogue access point detection: automatically detect and manage wireless threats to your network  
[http://www.proxim.com/learn/library/whitepapers/Rogue\\_Access\\_Point\\_Detection.pdf](http://www.proxim.com/learn/library/whitepapers/Rogue_Access_Point_Detection.pdf)
- [14] Shim, R. ZDNet: Canadian arrest highlights the dangers of Wi-Fi  
<http://insight.zdnet.co.uk/communications/wireless/0,39020430,39118205,00.htm>
- [15] TRENDnet' TEW-T1 2.4 GHz Wi-Fi Detector  
<http://www.trendnet.com/products/TEW-T1.htm>
- [16] Wenyuan, X., Trappe, W., Zhang, Y., Wood, T. The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing* (Urbana-Champaign, IL). ACM Press, New York, NY, 2005, 46 – 57.
- [17] Wi-Fi Alliance  
<http://www.wi-fi.org/>