

# Security and Fraud Risks of Internet Protocol-based Wireless Networks

a report by

**Jim L Elliot**

Board of Directors, Communications Fraud Control Association (CFCA)

## Introduction

All of the traditional telecoms fraud and Internet problems still exist in 2002. This article addresses the traditional and new risks associated with moving to Internet Protocol (IP)-based networks. In summary, the current 802.11<sup>1</sup> and Bluetooth™ standards possess vulnerabilities that make their usage questionable and the security of infrastructures are at stake.

## Wireless Networks

Wireless networks can be readily identified in most developed urban areas and neighbourhoods. In many business areas, identifying one new network per minute is the norm in late 2002 and the security problems start to surface when it is determined that most of these networks are running on the vendor-supplied 'default' with no security. With wireless cards for laptops selling for under US\$100, this accessing of available 'open networks' can be expected to continue. If one wants to create their own wireless network, the required 'access point' is available for under US\$200.

## War Dialling, War Walking and War Chalking

'War dialling' is a dated technique in which a hacker programs his/her system to call hundreds of telephone numbers in search of poorly protected computer dial-ups.

The practice of driving/walking through an area while using tools such as laptops to discover the beacons of wireless networks is known as 'war walking' (or 'war driving'). Using such a network does not even require special software or hardware; an ordinary consumer wireless card will latch on to the beacons and allow access to networks.

A more recent development is known as 'war

chalking'. This is the process of using chalk to place a special symbol on the side of a building, a pavement or other surface that indicates the presence of a nearby wireless network.

## Some of the Threats

Multiple potential threats exist against the telecoms infrastructures of today. The primary assumption is that the threat comes from outside the organisation and these threats will be addressed here. However, it should also be pointed out that the primary threat to infrastructures has repeatedly been found to be from within. Still, the outside threat does exist and, for wireless networks, is physically outside the physical perimeter of the wireless networks.

Assuming that the primary reason for accessing a wireless network is for anonymity, then many different groups such as terrorists, organised crime and protestors have a vested interest in being able to penetrate wireless networks. Other goals can be the disruption of corporate infrastructures and the wireless network clearly has the access required to achieve this goal.

## Some Wireless Fidelity (Wi-Fi) Characteristics

There exist several common characteristics between the various wireless standards. These include, but are not limited to, the following:

- The wireless standards in common use operate in the unlicensed industrial, scientific and medical frequency bands.
- The devices radiate low power.
- The range of operation is based on the specific specification, antenna design and path loss. The 'on-card antennas' provide a range of up to a few hundred feet, while an external antenna with line-of-sight has proven to allow distances of up to

Jim L Elliott is a Member of the Board of Directors of the Communications Fraud Control Association (CFCA) and also Spectrum Signal Processing. He is a member of the New York Electronic Crimes Task Force (NY ECTF) and an instructor at the Federal Law Enforcement Training Center (FLETC). In addition to these responsibilities, he is also an employee of Booz Allen and Hamilton. He has been working in the areas of telecoms fraud, infrastructure assurance and computer crime investigation since 1990 and his team is currently investigating the vulnerabilities and interoperability issues within cellular and Internet Protocol (IP)-based communications networks. Mr Elliott presents seminars and training to international law enforcement personnel, international telecoms carriers and military personnel in online investigative techniques, diagnosis and responses to telecoms fraud and network threats. He is an expert in the area of telecoms fraud and threats to public networks. Mr Elliott holds graduate and undergraduate degrees in Engineering and Computer Science from Oregon State University and Oklahoma State University, respectively.

1. 802.11 refers to a family of specifications developed by the Institute of Electrical and Electronics Engineers, Inc. (IEEE) for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997.

**Box 1: Brief IP Glossary**

- APNIC – Asia Pacific Network Information Center
- ARIN – American Registry for Internet Numbers
- AS – autonomous system. In the Internet model, an AS is a connected segment of a network topology that consists of a collection of sub-networks (with hosts attached), interconnected by a set of routes.
- BG – border gateway. A router between intra-performance monitoring network (PMN) and inter-PMN backbone networks. (For additional information, see Global Scheduling Multiple Access (GSMA) document IR.33).
- BGP – Border Gateway Protocol. An inter-AS routing protocol. The current version of BGP is BGP-4.
- DNS – Domain Name Service. For additional information, see GSMA document IR.33.
- Gateway/router – In the Internet model, constituent networks are connected by IP datagram forwarders, which are called routers or IP routers. Some Internet documents refer to routers as gateways. See also BG (border gateway).
- IPSec – Internet Protocol Security
- QoS – quality of service
- RIPE – Réseau IP Européens

**Box 2: Brief 802.11 Glossary**

- 802.10 – An IEEE standard establishing specifications for security in both wired and wireless local area networks (LANs).
- 802.11 – An IEEE standard establishing specifications for Wi-Fi communications.
- 802.11a – The next step in Wi-Fi technology. This specification allocates three 100 megahertz (MHz) sub-bands in the five gigahertz (GHz) region for unlicensed Wi-Fi use. Transmissions operate at speeds of up to 54Mhz.
- 802.11b – The current Wi-Fi technology. This specification allocates three 100MHz sub-bands in the 5GHz region for unlicensed Wi-Fi use. Transmissions operate at speeds of up to 11Mhz.
- Access Point (AP) – Hardware that connects a Wi-Fi LAN to an existing wired network. There can be multiple access points in a large office, overcoming the transmission distance limitations of Wi-Fi and permitting users to roam with their laptops throughout (and outside) a large building while remaining connected to the Wi-Fi LAN.
- Bluetooth™ – A wireless standard that never really caught on with the consumer. In contrast to Wi-Fi, which easily extends hundreds of feet (and further with specialised equipment), Bluetooth is intended for appliance-to-appliance communication of not more than 30 feet. Bluetooth is also far slower than Wi-Fi. A typical Bluetooth communication involves a Bluetooth-enabled personal digital assistant that automatically synchronises with a desktop personal computer.
- Industrial, Scientific and Medicine Bands (ISM Bands) – The 2.4GHz band is one of three bands known as the ISM frequency bands – for industrial, scientific and medical applications, which has the potential to be somewhat crowded. The Federal Communications Commission (FCC) allocated 902MHz, 2.4GHz and 5.7GHz for these purposes.

- Wireless Ethernet Compatibility Alliance (WECA) – An industry organisation promoting and certifying Wi-Fi products. Members include Zoom, 3Com, Dell, Aironet, Agere, Nokia and Nortel.
- Wired Equivalent Privacy (WEP) – An optional IEEE 802.11 security technology that has failed in that it has been cracked. ‘Wired equivalent’ refers to the claim that this Wi-Fi security is as good as wired networks enjoy. One thing that the comparison seems to ignore is that there is no physical barrier in Wi-Fi (e.g. a hacker can sit outside an office building and receive the office’s Wi-Fi transmissions). Beyond that, WEP is inherently flawed for several reasons, not least of which is that Wi-Fi passwords are usually static (for convenience, users continue to use the same password instead of changing it periodically). For an in-depth report on the collapse of WEP security, see S Fluhrer, I Mantin, A Shamir, “Weaknesses in the Key Scheduling Algorithm of RC4”, *Lecture Notes in Computer Science*, 2,259 (2001). See also Chapter 8: *Security and Encryption*, for details about AirSnort and other WEP attackers. AirSnort, for example, requires that between roughly 100 megabytes and one gigabyte of Wi-Fi data be captured (by someone outside a building). Once sufficient data has been gathered, AirSnort requires less than one second to compute the encryption password being used.

several miles. Obstacles in the line-of-sight path (e.g. walls, trees, buildings) are the key factors affecting range. It may be, surprisingly, that rain also has the ability to impact the effective distance over which a network can operate.

**Quality of Service is Needed**

As the industry evolves from circuit-switched to packet-switched networks and the users move more towards using voice over IP (VoIP) and other realtime communications (e.g. streaming multimedia), a quality of service (QoS) will be mandated to satisfy customer needs. The new 802.11e specification could overlay several different Institute of Electrical and Electronics Engineers, Inc. (IEEE) standards, including 802.11b, 802.11g and 802.11a.<sup>2</sup>

**802.11 versus GPRS/UMTS**

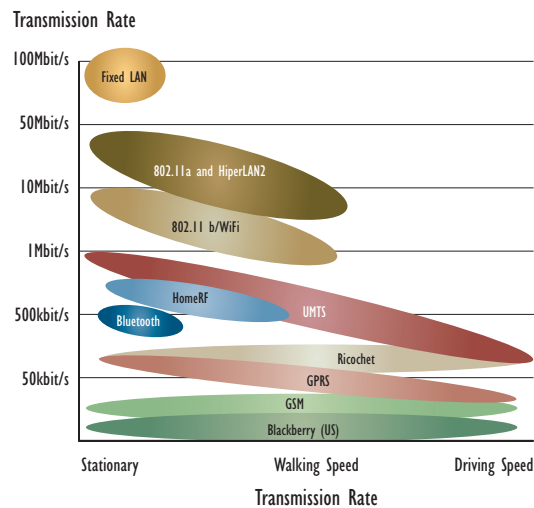
As illustrated in *Figure 1*, the cellular 2.5G/GPRS and the 3G/UMTS™ offer data rates that are lower than the existing 802.11 standard. This then can easily put the two technologies in competition with each other.

**Improving Wireless Security**

Though the wireless networks have many security problems, these can be managed. The following items will help increase the security of existing and planned wireless networks:

1. Keep 802.11 outside the firewall – the wireless access network should be viewed as just an ‘access node’ and a user should still be required to access the corporate infrastructures with all the other existing accesses. Often, the problem is that the

**Figure 1: 802.11 versus GPRS/UMTS**



Source: Monica Paolini, “Public Wireless LAN Access: A Threat to Mobile Operators?”, TotalTelecom Reports, August 2001, <http://www.totaltele.com/reports/default.asp?report=pwla>

wireless access node has been connected to the network in such a way that the normal access mechanisms have been circumvented.

2. 802.11x is a version of the standard that hopes to solve many of the security issues.
3. Use of some vendor-specific advancements – some vendors have vendor-specific solutions that have been found to solve some of the security issues.
4. Use of Wired Equivalent Privacy (WEP) with 128-bit keys and frequent changes – the WEP feature is built in to the 802.11 protocol. Unfortunately, many users make no use of this feature and networks are left vulnerable.

2. Further explanation of this is covered by the 802.11 Task Group Update with documents available on the website: <http://www.oreillynet.com/pub/a/wireless/2002/04/05/80211taskgroups.html>

### Future Problems

If these problems were not enough, as mobile networks move forward, the devices will be 'always on'. This adds infrastructure build-out and support problems to already debt-burdened carriers. All of the existing IP problems will also migrate to the wireless networks and the law enforcement challenges will still exist. This migration to IP-based networks will also result in the need for a new approach to billing, which is based either on 'data-rate' and/or on QoS level instead of the existing distance and time parameters.

### Conclusions

As more and more networks become IP-based, these problems will continue, though some will only want connectivity; traditional public-switched telephone networks running on circuit-switched networks, and even telex networks, are still functional and still provide reliable communications. Fortunately, several vendors offer products that help with intrusion detection, QoS and lawful legal interception problems. Steps should be taken to try to protect against the threat and the vulnerabilities will take care of themselves. ■

### References

- N Borisov, I Goldberg and D Wagner, "Security of the WEP Algorithm", 2001  
<http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>
- Walter R Bruce (2002), *Wireless LANs End to End*, Ron Gilster (ed.), John Wiley & Sons.
- Harold Davis and Richard Mansfield (2001), *The Wi-Fi Experience: Everyone's Guide to 802.11b Wireless Networking*, Que.
- S Fluhrer, I Mantin, A Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", *Lecture Notes in Computer Science*, 2,259 (2001).
- Marcus Goncalves and Kitty Niles (2001), *IPv6 Networks*, McGraw-Hill.
- Stuart McClure, Joel Scambray and George Kurtz (2001), *Hacking Exposed: Network Security Secrets & Solutions*, (3rd ed.), McGraw-Hill Osborne Media.
- Harry Newton (2002), *Newton's Telecom Dictionary: The Authoritative Resource for Telecommunications, Networking, the Internet and Information Technology*, (18th ed.), CMP Books.
- Stephen Northcutt, Donald McLachlan and Judy Novak (2000), *Network Intrusion Detection: An Analyst's Handbook*, (2nd ed.), New Riders Publishing.
- A Stubblefield, J Ioannidis and A D Rubin, "Using the Fluhrer, Mantin, Shamir Attack to Break WEP", (Revision 2), AT&T Laboratories Technical Report TD-4ZCPZZ, 21 August 2001, [http://www.cs.rice.edu/~astubble/wep/wep\\_attack.pdf](http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf)