

Background

This technical note is intended to inform readers about UK Government policy on Wireless Local Area Networks (WLANs). This technical note contains technical background on the nature of the vulnerabilities and the best means of mitigating their impact.

Summary

The UK Government shares the view of the commercial security industry that WLANs conforming to the existing IEEE 802.11 standard are extremely likely to be insecure. The aspects of security affected are the privacy, confidentiality and integrity of data transmitted across a WLAN, all connected devices or networks, and availability of the WLAN itself. The weaknesses in privacy and confidentiality relate to well-publicised vulnerabilities in the Wired Equivalency Privacy (WEP) protocol used to provide data link layer encryption. Moreover, the risks to privacy of data extend to wired systems connected to WLANs via wireless access points, as wireless access points are often configured by default not to use authentication mechanisms and hence can be used to gain illegitimate access to wired networks. The integrity of information from WLANs may have been compromised and should not be treated as trusted or genuine. It is possible to capture data in transit and to alter that data without detection by the integrity checker. The threat to availability is that a wireless connection can be blocked by Radio Frequency (RF) jamming or by deliberate RF transmission.

The vulnerabilities in WLANs can be exploited with inexpensive equipment that can be constructed using freely available instructions. These exploits can be carried out at considerable distances from the WLAN wireless access point, depending on the configuration of the network and the antennas deployed. Given that a number of tools available on the Internet exist to simplify attacks on WLANs, attackers need minimal sophistication. The availability of the equipment together with the simplicity of attacks in practice has led to unauthorised WLAN access becoming a common pastime amongst hackers (see <http://www.netstumbler.com>)

In light of the existence of these classes of vulnerability and their ease of exploitation, decisions to use wireless technology should explicitly determine whether the business benefits are sufficient to outweigh the possible consequence of exploitation. The UK Government's conclusion is that most Government data is unsuitable for transmission across WLANs unless that data is also encrypted by a method approved by CESG, the UK national cryptography authority.

The situation is liable to change because work is ongoing in the IEEE on the 802.11i standard (Media Access Control Enhancements for Enhanced Security) to resolve the cryptographic vulnerabilities discussed below. Use of the IEEE 802.1x port-based authentication standard in wireless network implementations may also increase security, although theoretical security vulnerabilities have already been discovered.

What is IEEE 802.11?

IEEE 802.11 is a standard for "wireless connectivity for fixed, portable, and moving stations within a local area" [1]. IEEE 802.11 applies at the lowest two layers of the Open System Interconnection (OSI) protocol stack, namely the physical layer and the data link layer. The physical layer standard specifies the signalling techniques used and the implementation of media specific functions. The data link layer defines the frame transmission structure for control, data and management messages and the architecture for data transmission across a WLAN. Key notions are those of association, which is the mapping of wireless clients to a wireless access point, and of service set, which is a set of co-ordinated wireless clients that can be regarded as analogous to a wired network segment.

Included in the IEEE 802.11 standard is the requirement to provide for privacy of data transmission across wireless networks. The way that privacy is provided is by use of the WEP [2]. WEP is a protocol that uses RSA's RC4 data stream encryption and CRC-32 integrity checking of data frames at the data link layer. WEP is usually implemented in the hardware and firmware of the wireless network interface cards. It is worth stressing that vulnerabilities in WEP will require a new generation of wireless interface cards.

Current standards for WLANs are IEEE 802.11a (high speed 5 GHz WLANs) [3] and 802.11b (high speed 2.4 GHz WLANs) [4]. IEEE 802.11a and 802.11b are incompatible standards (specifying different physical layers and transmission frequencies), and to date commercial implementations of IEEE 802.11b have been far more widespread. As noted above, deficiencies in the security of 802.11 have stimulated the development of IEEE 802.11i [5] for an enhanced data link layer WLAN encryption standard. However, the 802.11i standard is still under development and is not likely to be finalised before the end of 2003. Use of the IEEE 802.1x [6] standard for port based access control also seemed promising, but theoretical vulnerabilities (a session hijacking and a man in the middle attack) were discovered in the application of IEEE 802.1x to 802.11 [7]. These vulnerabilities use, respectively, the ability to spoof a disassociation message from a wireless access point to a wireless client whilst maintaining authenticated status for the session and the ability of a third-party to spoof a successful authentication message on behalf of the wireless access point.

Security Measures & Vulnerabilities

A significant problem with WLANs, as with many other type of product, is that many of them have insecure default configurations, enabling attackers to connect without authentication. However, many current implementations of IEEE 802.11 WLANs can be configured to provide some or all of the following security measures.

- Service Set Identifier (SSID)
- Media Access Control (MAC) filtering
- WEP

The SSID is used to specify the name of a network segment related to a set of wireless access points. The SSID is used as a simple authentication token for a wireless access point. It should therefore be changed from the factory default. However the SSID has limited value as a security measure. A wireless client identifies available access points by sending a probe request frame. By sending a probe request with an SSID of 0 ("a broadcast SSID"), which is often implemented by as an "Any" entry in the SSID field on the client, a wireless access point will by default respond by sending its SSID(s). Responses to broadcast SSID probe requests should, if possible, be disabled on the access point. The access point will then only respond to probe requests with the correct SSID(s) for the access point. This measure will not prevent collection of SSID(s), as the access point will also transmit its SSID(s) in beacon frames periodically. However, it may be possible to disable the transmission of beacon frames (eg by setting the beacon interval to zero).

The MAC address of a network interface card is used to identify the interface card. By restricting the MAC addresses that can connect to a wireless access point it is possible to provide some access control. However, because the MAC address is sent in clear in

the data link layer header, it can be obtained by network monitoring and the MAC address of an attacker's wireless network card altered to correspond to it (known as MAC address spoofing).

It is also possible to poison the Address Resolution Protocol (ARP) cache used to relate computers' MAC network interface card addresses to IP addresses via the wireless access point [8]. The attacker can send a crafted ARP reply packet that maps the IP addresses of other hosts to the MAC address of his machine. Such an attack would enable the attacker to intercept traffic routed through his computer and potentially to modify the traffic en route.

WEP has been the subject of a great deal of analysis. It has the following fundamental problems:

- All clients and the wireless access point share the same secret key, which is used to generate each RC4 cipher stream
- The initialisation vector used (concatenated with the secret key) to generate the RC4 cipher stream is transmitted in clear
- The initialisation vector is too short at 24 bits
- The integrity check algorithm, CRC-32, is non-cryptographic

Owing to the way that RC4 works, it is possible to perform a logical exclusive "or" operation on two cipher streams generated with the same initialisation vector and secret key and to generate the exclusive "or" of the original plain texts [9]. By collecting sufficient traffic, it is possible to determine the original plain texts. It is also possible by collecting sufficient traffic with initialisation vectors satisfying certain conditions to determine the value of the shared secret key [10, 11]. The success of these attacks relies on the transmission of the initialisation vector in clear, the existence of a common secret key, and, to a varying extent, on the length of and randomness of the initialisation vector.

Due to the non-cryptographic nature of the CRC-32 integrity checker and the RC4 decryption process, it is also possible to alter the WEP encrypted data in such a way that alterations will not be detected. The integrity of wireless data thus cannot be guaranteed (see [9]).

Exploitation of vulnerabilities

As noted in the executive summary, these attacks on WEP have been implemented in practice, and tools using these techniques are readily available on the Internet that decrypt WEP encrypted data frames. To the best of our knowledge, however, there are no tools available to perform WEP encrypted frame modification or exploitation of the session hijacking or man in the middle attacks on IEEE 802.1x.

Mitigation & Remediation

Given the ease of exploitation of the vulnerabilities in WEP, the recommended course of action is to avoid the use of WLANs unless there is a strong business case.

In the event that there is a business requirement for WLANs, risks may be mitigated by:

- Enabling all security features of the WLAN
- Providing a virtual private network to provide end-to-end encryption of all traffic to and from computers on the wired LAN across the WLAN
- Restricting the wireless network to the organisation's property
- Place access points (APs) inside your organisation's physical perimeter and use directional antennae in such a way as to reduce stray RF radiation [12]

Specific configuration steps that may be available include:

- Changing the SSID from the default
- Disabling APs from broadcasting their SSIDs
- Disabling APs from responding to broadcast probe requests
- Enforcing MAC address filtering
- Enabling WEP
- Changing the shared secret key regularly

As an alternative to a virtual private network, it may be appropriate to install a third-party authentication server that sits on the wired LAN behind the wireless access point and distributes keys dynamically to validated system users. This type of authentication server is a key component of the IEEE 802.1x protocol, and it helps to address some of the key management problems of WEP as well as providing access control to wired LANs. This standard is currently implemented in some wireless products. If this strategy is adopted, the existence of session hijacking and man in the middle vulnerabilities in IEEE 802.1x when used with IEEE 802.11 need to be taken into account as part of the risk management strategy. Theoretically the effect is that an attacker could take over an established session or relay traffic through a third-party computer. There are currently no mitigating steps for these vulnerabilities.

There is a need for an assured secure WLAN product. For Government use, a product formally assured by CESG under the CAPS (CESG Approved Products Scheme) is recommended for low sensitivity data and is mandatory for higher sensitivity data. No such product has yet been assured, although one vendor has started to submit a product for evaluation. Furthermore, a CAPS approved product, Barron-McCann's X-Kryptor, which consists of a TCP/IP encryption gateway and client device driver, has been assured for the communication of up to RESTRICTED data (see <http://www.cesg.gov.uk/partnerships/pwi/caps/capsprods.htm>) and can be used to provide secure end-to-end virtual private networks across WLANs.

Because wireless networks currently need to be treated as insecure, firewalls should be used to separate wireless networks from

wired networks and to filter all traffic sent to the wired network. Another reason for the use of a firewall is to prevent the virtual private network being bypassed by requesting other network services. If WLAN clients are assigned dynamic IP addresses, there may be a need to allow Dynamic Host Configuration Protocol (DHCP) requests and responses through the firewall. In this case a state aware firewall should be used which is capable of blocking flooding attacks against the DHCP server.

ARP spoofing is also still a concern even if a virtual private network is deployed. For this reason, the use of a firewall or a screening router is recommended. (Routers and firewalls strip out the data link layer, including the MAC address.)

A possible architecture to minimise risk to the security of data transmitted between wired network segments is:

```
Wired LAN segment <->
Firewall <->
Screening router <->
IP encryption device <->
Wireless access point <->
WLAN <->
Wireless access point <->
IP encryption device <->
Screening router <->
Firewall <->
Wired LAN segment
```

For wireless clients communicating with a wired network segment a possible architecture is:

```
Wired LAN segment <->
Firewall <->
Screening router <->
IP encryption device <->
Wireless client with virtual private network software
```

It should be noted that wireless clients are still liable to denial of service attack by spoofing a disassociation message from a wireless access point.

Further Information

Further advice and information can be obtained from the following sources:

The Manual of Protective Security as amended by S(E)N 02/04 [13] for UK Government departments

The NISCC outreach team (available via the NISCC help desk, tel: 0207 821 1330 x4511, email:enquiries@nisc.gov.uk) for UK CNI organisations

The Home Office Press Office (tel: 020 7273 4545) for press enquiries

For advice on solutions appropriate to a particular system, Government departments are advised to contact CESG consultants, or, for less sensitive requirements, CESG Listed Advisers (look for CLAS membership on the CESG web site,<http://www.cesg.gov.uk/partnerships/pwi/clas/index.htm>). A text reference on wireless networks is "802.11 Wireless Networks: The Definitive Guide" [14].

Notes & References

The inclusion of the references below does not constitute NISCC verification of accuracy or endorsement of the advice contained in these references. They are cited for information only.

[1] ANSI/IEEE Std 802.11, 1999 Edition, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. (see: <http://standards.ieee.org/getieee802/802.11.html>) Section 1.1, p1

[2] ANSI/IEEE Std 802.11, 1999 Edition, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Section 8.2, pp62-65.

[3] IEEE Std 802.11a-1999 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band (see: <http://standards.ieee.org/getieee802/802.11.html>)

[4] IEEE Std 802.11b-1999 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band (see: <http://standards.ieee.org/getieee802/802.11.html>)

[5] See: http://grouper.ieee.org/groups/802/11/Reports/tgi_update.htm

[6] IEEE Std 802.1X-2001 Port-Based Network Access Control (see: <http://standards.ieee.org/getieee802/802.1.html>)

[7] An Initial Security Analysis of the IEEE 802.1X Standard, A.Mishra & W.A.Arbaugh, Department of Computer Science, University of Maryland, College Park (see: <http://www.cs.umd.edu/~waa/1x.pdf>)

[8] Wireless Access Points and ARP Poisoning: Wireless vulnerabilities that expose the wired network, R.Fleck & J.Dimov, Cigital Inc., 2001, (see: <http://www.cigitalabs.com/resources/papers/download/arppoison.pdf>)

[9] Intercepting Mobile Communications: The Insecurity of 802.11, N. Borisov, I. Goldberg & D. Wagner (see: <http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf>)

[10] Weaknesses in the Key Scheduling Algorithm of RC4, S. Fluhrer, I. Mantin & A. Shamir (see: http://downloads.securityfocus.com/library/rc4_ksaproc.pdf)

[11] Using the Fluhrer, Mantin and Shamir Attack to Break WEP, A Stubblefield, J.Ioannidis and A.D.Rubin. August 21, 2001 (see: http://www.cs.rice.edu/%7Eastubble/wep/wep_attack.pdf)

[12] Antennas Enhance WLAN Security, T. Marshall. 1 October 2001 (see: http://www.byte.com/documents/s=1422/byt20010926s0002/1001_marshall.html)

[13] Electronic Information Processing Security Notice S(E)N 02/4, Revised Policy on Wireless LANs, Cabinet Office, 30 April 2002

[14] 802.11 Wireless Networks: The Definitive Guide. Creating and Administering Wireless Networks. M. Gast. April 2002 (O'Reilly ISBN 0-596-00183-5)