Global Information Assurance Certification Paper

Incident Handling & Hacker Exploits Practical assignment version 1.5c option 2

Wireless LAN honeypots to catch IEEE 802.11 intrusions: a discussion of vulnerabilities and a solution

By Gordon L. Mitchell, PhD, CISSP
June 29, 2001

Contents

Introduction

The use of wireless networks has accelerated in the last year. Reasons are clear to those who enjoy the benefit of answering e-mail in a dull meeting, connecting to the network from an unwired office or just being able to move an untethered laptop around at home.

Typical wireless LAN configurations are designed to meet a standard for systems that work in the 2.4 Gigahertz band. The 802.11 standard can be implemented in infrared systems also but this transmission medium is rarely used. The radio-based devices are operated as unlicensed transmitters in many countries and use common techniques for modulation / demodulation of signals. More of these radio aspects are described in a previous paper.[1]

This combination of standards and easily intercepted radio transmissions produce a significant vulnerability if security precautions are not taken. The risk is particularly great because a new cult of (ultra) short wave listeners is following the installation of wireless networks. All they need to listen in to many networks is a $150 wireless LAN card and a laptop. The results are well publicized and require little expertise to implement.

Solutions to these vulnerabilities are obvious. Don't reuse passwords over wireless LANs, encrypt traffic to foil wireless LAN sniffers and prohibit wireless networks for the most sensitive material. In practice each of these presents significant administrative difficulties; in some situations they just don't work.

The question remains, "How do I know if someone is sniffing my wireless traffic?" This paper presents a solution to that concern using an access point configured to attract and monitor intrusions – *a wireless honeypot*.

Exploit details

Name: Wireless LAN sniffing/intrusion
Variants: Sniffing wireless traffic, gathering information to break the (poorly designed) encryption of standard 802.11 wireless networks, denial of service by alteration of Access Point settings. All of these variants can be deployed without touching the wired network which is attached to the wireless system. If the wired network can be accessed, however, the attack against a wireless system can be even more devastating.
Operating System: Any OS with wireless LAN attached.
Protocols/Services: Same as an intruder can access by connecting to the Ethernet serving a wireless Access Point. Note, this connection often allows inside-the-firewall access to an otherwise secure network.
Brief Description: The worst case vulnerability is a wireless network with no

encryption. This happens when Access Points (APs) are configured without Wireless Equivalent Privacy (WEP) selected and when no end-to-end encryption such as SSH or connections run over SSL is used.

When this happens an intruder only needs to be within the range of an AP with a wireless network card preset to a blank Extended Service Set Identity (ESSID). The intruder's computer will then connect (Associate) to the AP. This situation is essentially like plugging into a data jack except that it can be done by an intruder in the parking lot!

Typical wireless LAN card in a laptop – the only equipment that an intruder needs to connect to an unprotected network access point. Sniffers, scanners and protocol analyzers may also be used to conduct various attacks with this setup. [2]

Even when WEP is enabled intruders can capture wireless packets for later analysis. Often this weak encryption system can be defeated with pencil and paper -- not needing significant computer power.

The final insult is that wireless plaintext intercepts may be legal in most jurisdictions. This is because they are as public as any radio transmission by a public service agency or taxicab company. Some privacy laws protect communications between people but would this include checking a book order on a web site?

In light of this threat it is important to take countermeasures that alert wireless network operators of intrusion attempts. A wireless honeypot which accomplishes this is described later in this document.

Protocol Description

Wireless networks considered in this paper conform to IEEE Standard 802.11[3]. Typical commercial installations of these networks have:

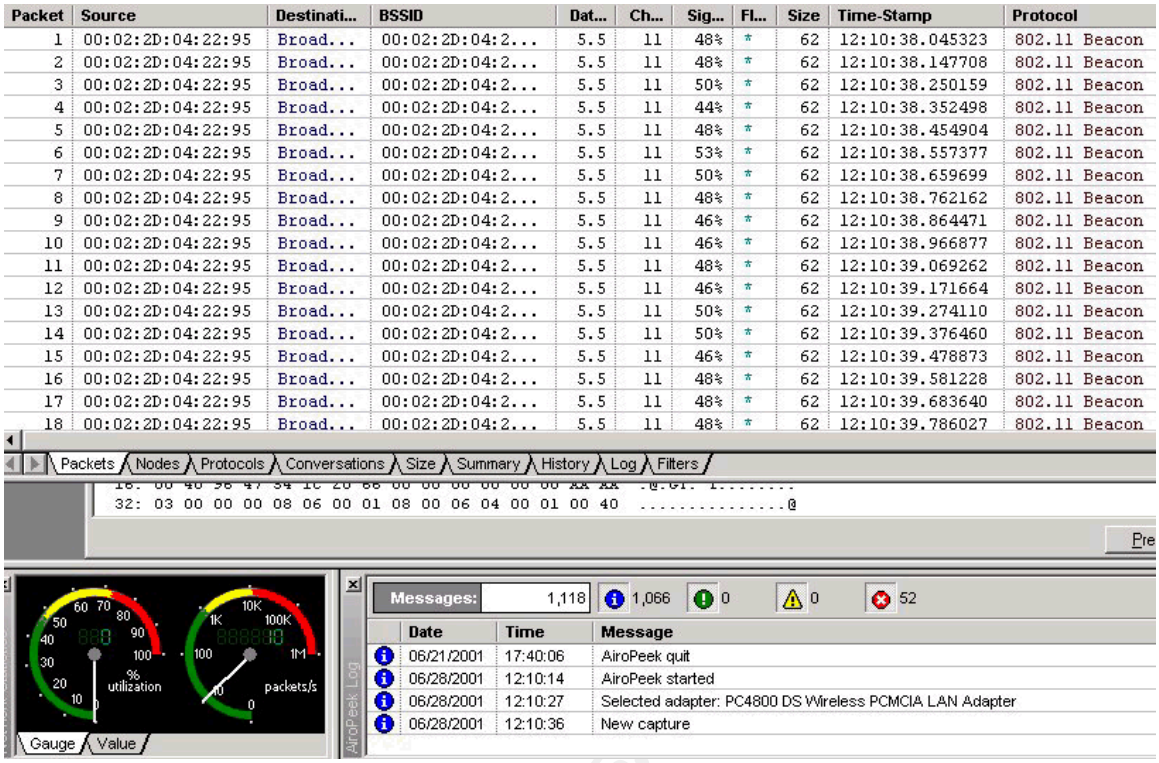
- A number of Access Points (APs) above the drop ceiling
- Ethernet connections between the APs and the building's wired network
- Laptops with PC cards which communicate to the APs
- A scheme for distributing secret keys if encrypted operation is desired

When the APs are installed they are configured by

- Assigning an IP address
- Entering any secret key(s) that will be needed
- Setting radio parameters related to the channel of operation, antenna diversity, power levels,…
- Selecting security features such as AP passwords, user access control lists, and the modes of operation that will allow changing AP parameters.

Once APs are in service on an Ethernet connection remote monitoring is possible via standard SNMP or proprietary systems. Features build into the AP firmware allow changing system configuration via telnet or a built in web server.

When APs are powered up they transmit beacon signals to prospective mobile users. Normally these beacon signals are sent out 10 times per second. They include an Extended Service Set ID (ESSID) which is not a security measure but does allow nearby wireless networks to avoid connections to another organization's mobile users. Beacon signals from a typical AP are shown in the screen shot below



Packet	Source	Destinati...	BSSID	Dat...	Ch...	Sig...	Fl...	Size	Time-Stamp	Protocol
1	00:02:2D:04:22:95	Broad...	00:02:2D:04:2...	5.5	11	48%	*	62	12:10:38.045323	802.11 Beacon
2	00:02:2D:04:22:95	Broad...	00:02:2D:04:2...	5.5	11	48%	*	62	12:10:38.147708	802.11 Beacon
3	00:02:2D:04:22:95	Broad...	00:02:2D:04:2...	5.5	11	50%	*	62	12:10:38.250159	802.11 Beacon
4	00:02:2D:04:22:95	Broad...	00:02:2D:04:2...	5.5	11	44%	*	62	12:10:38.352498	802.11 Beacon
5	00:02:2D:04:22:95	Broad...	00:02:2D:04:2...	5.5	11	48%	*	62	12:10:38.454904	802.11 Beacon
6	00:02:2D:04:22:95	Broad...	00:02:2D:04:2...	5.5	11	53%	*	62	12:10:38.557377	802.11 Beacon
7	00:02:2D:04:22:95	Broad...	00:02:2D:04:2...	5.5	11	50%	*	62	12:10:38.659699	802.11 Beacon
8	00:02:2D:04:22:95	Broad...	00:02:2D:04:2...	5.5	11	48%	*	62	12:10:38.762162	802.11 Beacon
9	00:02:2D:04:22:95	Broad...	00:02:2D:04:2...	5.5	11	46%	*	62	12:10:38.864471	802.11 Beacon
10	00:02:2D:04:22:95	Broad...	00:02:2D:04:2...	5.5	11	46%	*	62	12:10:38.966877	802.11 Beacon
11	00:02:2D:04:22:95	Broad...	00:02:2D:04:2...	5.5	11	48%	*	62	12:10:39.069262	802.11 Beacon
12	00:02:2D:04:22:95	Broad...	00:02:2D:04:2...	5.5	11	46%	*	62	12:10:39.171664	802.11 Beacon
13	00:02:2D:04:22:95	Broad...	00:02:2D:04:2...	5.5	11	50%	*	62	12:10:39.274110	802.11 Beacon
14	00:02:2D:04:22:95	Broad...	00:02:2D:04:2...	5.5	11	50%	*	62	12:10:39.376460	802.11 Beacon
15	00:02:2D:04:22:95	Broad...	00:02:2D:04:2...	5.5	11	46%	*	62	12:10:39.478873	802.11 Beacon
16	00:02:2D:04:22:95	Broad...	00:02:2D:04:2...	5.5	11	48%	*	62	12:10:39.581228	802.11 Beacon
17	00:02:2D:04:22:95	Broad...	00:02:2D:04:2...	5.5	11	48%	*	62	12:10:39.683640	802.11 Beacon
18	00:02:2D:04:22:95	Broad...	00:02:2D:04:2...	5.5	11	48%	*	62	12:10:39.786027	802.11 Beacon

Access Point beacon broadcasts shown here as received by a wireless LAN sniffer AiroPeek [4]

In the packet capture shown above items of interest include

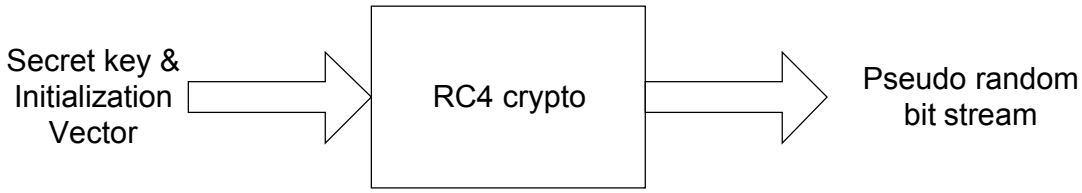
- The source is the MAC address of the PC card in the AP; this address is also the Broadcast Service Set ID (BSSID).
- In this case the raw data rate is 5.5 megabits per second, actual throughput (excluding overhead and dead air) will be about half of this rate.
- The received signal strength is shown as a percentage of the signal strength which would be realized with the AP and mobile user a meter or so apart.

The details of network operation as well as the various options for transmission of data are covered in a summary paperback by O'Hara and Petrick[5]

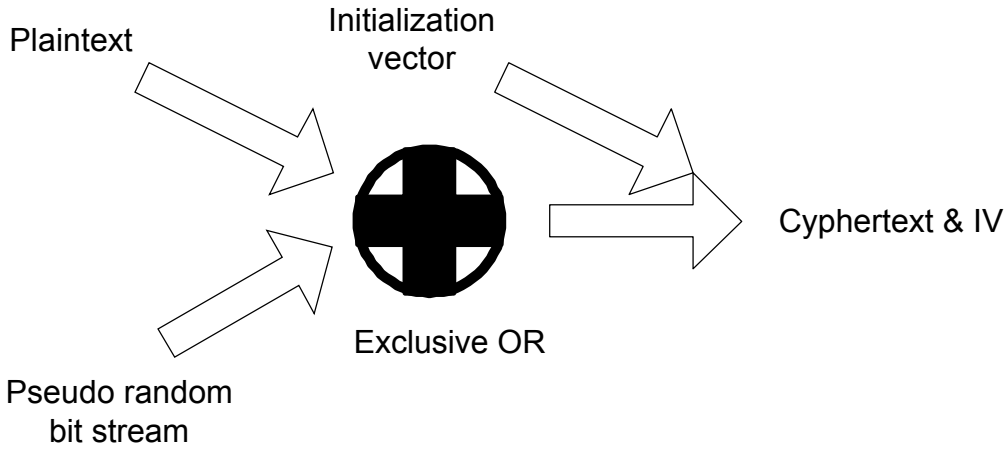
An important part of the protocol involves encryption to achieve Wired Equivalent Privacy (WEP). The technology chosen was clearly a compromise between something that would work with limited computational power of a PC card and something that would produce a bulletproof cryptosystem. The tradeoffs in this design were real. Early (circa 2000) wireless PC cards failed because of the heat generated by onboard circuitry.

The choice for data encryption and user authentication was RC4[6], a respected stream cipher. RC4 can be implemented with almost an order of magnitude less computation than an equivalent Digital Encryption Standard (DES) algorithm.

In 802.11 WEP is accomplished by combining a pseudo random sequence with the data to be encrypted (plaintext). This is illustrated in the diagrams below.



First a 24 bit initialization vector, which may be regenerated for each frame, is appended to the 40 or 128 bit secret key. This is used to generate a pseudo random bit stream that is as long as the plaintext to be encrypted. This pseudo random bit steam is used to conceal the plaintext by a simple exclusive-or operation which produces cyphertext.



After the exclusive-or the initialization vector (IV) is appended to the cyphertext so it is available at the receiver for reversing this process. When the 802.11 standard was written a weakness in this process was recognized.

> When choosing how often to change IV values, implementors should consider that the contents of some fields in higher-layer protocol headers, as well as certain other higher-layer information, is constant or highly predictable. When such information is transmitted while encrypting with a particular key and IV, an eavesdropper can readily determine portions of the key sequence generated by that (key, IV) pair. If the same (key, IV) pair is used for successive MPDUs, this effect may substantially reduce the degree of privacy conferred by the WEP algorithm, allowing an eavesdropper to recover a subset of the user data without any knowledge of the secret key. Changing the IV after each MPDU is a simple method of preserving the effectiveness of WEP in this situation.[7]

Unfortunately some early PC cards used for APs and mobile users did not change the IV. As noted above this results in a situation which can easily be exploited by an

eavesdropper.

Authentication is generally considered to be a good security feature. Unfortunately in the 802.11 standard it actually decreases security.

From the standard:

> The required secret, shared key is presumed to have been delivered to participating STAs via a secure channel that is independent of IEEE 802.11. This shared key is contained in a write-only MIB attribute via the MAC management path. The attribute is write-only so that the key value remains internal to the MAC.
>
> During the Shared Key authentication exchange, both the challenge and the encrypted challenge are transmitted. This facilitates unauthorized discovery of the pseudorandom number (PRN) sequence for the key/IV pair used for the exchange. Implementations should therefore avoid using the same key/IV pair for subsequent frames[8].

The subtle wording here does not adequately describe the situation. In more direct terms the vulnerability here is that an eavesdropper can determine the pseudo random sequence for a particular IV. Since there are only 2^{24} possible IVs reuse is likely. This directly exposes plaintext.[9]

Description of variants

Variants of wireless network attacks are described in broad terms. Each of these variants can be implemented in a number of flavors. For example, the first is simply surveillance of an operating network which is not employing WEP. This can be accomplished using commercial products which are designed for network debugging such as AiroPeek. It can also be implemented with Linux utilities which put a wireless network card into a promiscuous mode. Wireless hardware manufacturers also have specialized sniffers.

In the following variants, WEP on implies an AP configured to only accept mobile users who have a correct secret key set into their wireless PC card. If the AP is set to operate in a mixed mode (users who have WEP enabled or not) all exploit variants can be used.

Direct sniffing – WEP off

When WEP is off, all network traffic as well as transmitted data is available to a wireless sniffer. This surveillance is also helpful for an intruder who wants to discover MAC addresses of legitimate users. If the AP has implemented an access control list only allowing certain MACs to associate it is possible to use sniffed information to assume the identity of an approved user.

Traffic analysis – WEP on

Even though data packets are not easily accessible, information about network activity, specific MAC addresses and packet length is available.

Decryption of encrypted packets – WEP on

Certainly it is possible to break 40 bit RC4 by a brute force attack, trying each of the (on average) 2^{39} necessary key possibilities. The attacks considered here are much simpler. For example, they may involve sending chosen plaintext which can be exclusive-ored with the corresponding transmitted cyphertext. This yields the pseudo random sequence (output of RC4) for the IV that has been used by the AP for this transmission.

AP hijacking

Most APs provide a simple web interface for easy setup. Often this interface can be accessed from the wireless side. If default passwords are used AP parameters can be observed or changed. This process requires knowing the IP address of the AP but that can be accomplished by scanning a range of addresses for port 80 (HTTP) responses. The web server in the AP will be listening on port 80 unless this AP feature has been disabled.

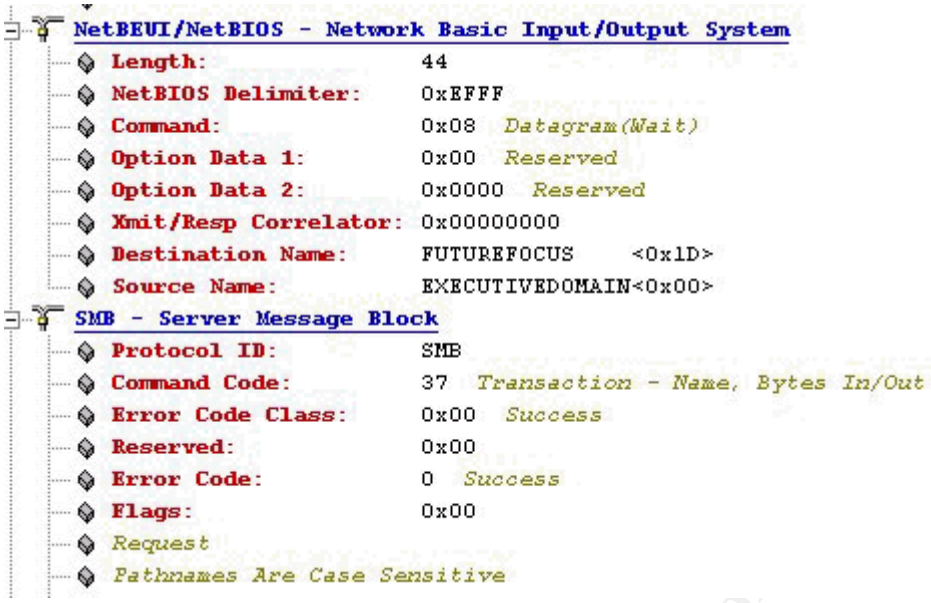
Wired network attacks

If an AP can be accessed via wireless it provides a window for exploitation of the attached wired network. Once an association with the AP is complete conventional scanners or other network probes can be deployed against the network.

How the exploit works

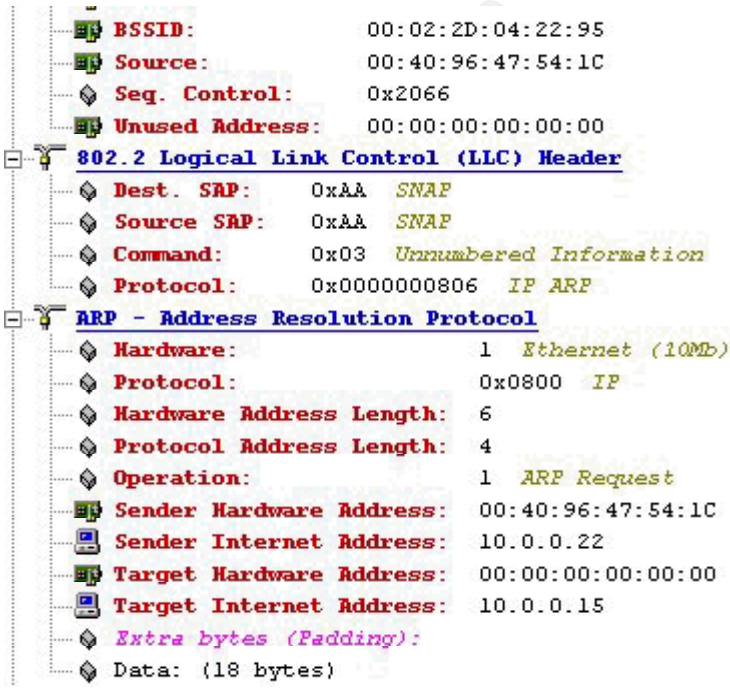
Direct sniffing – WEP off

The following screen capture from the wireless Ethernet sniffer AiroPeek illustrates information that is available to any radio receiver. This exploit only requires a wireless network card (about $150) and a laptop to implement.



This network information is from a staged intrusion which is described later in this document. This information includes the name of the workgroup and computer which are attached to a honeypot.

The following capture shows even more information.



Here IP addresses are shown. With this information an intruder could begin to gather information about the workstations, servers and routers that are visible from the wire that

the AP is connected to.

Traffic analysis – WEP on

IP headers are concealed when WEP is enabled but all MAC addresses are visible. General network activity can be discerned. Some APs for example will have only beacons present.

Decryption of encrypted packets – WEP on

Because of the short 24 bit IV the number of pseudo random RC4 outputs is limited to 2^{24}. This allows discovery of plaintext with a variety of methods. Attacks of this sort have been discussed in references[10]

If the identity of a workstation on the wireless network is identified a known plaintext attack can be used. Sending a relatively large, say 1500 byte, text block will allow directly discovering the pseudo random sequence for an IV. This means that all subsequent transmissions using this IV not larger than 1500 bytes can be directly decoded. If the same IV is used for all transmissions (the case in perhaps 10% of installations made in 2000) *all* wireless traffic from a given AP is easily decoded.

Of course the other option is to crack the crypo by brute force. If the 40 bit secret key is used this requires about 10^{12} RC4 trials.

AP hijacking

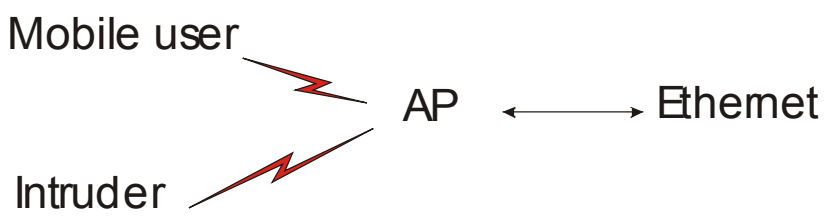
If an IP range for the network is noted (using a sniffer on unencrypted traffic) it is possible to guess what the IP assigned to the AP might be. A simple scan of an address range for port 80 will yield the IP address of an unprotected AP.

The next step is to point a browser at the IP address of the AP. This will connect to the built in web browser. If the AP password has not been changed from the default value it is possible to alter all settings. This can be used as a denial of service attack or to discover WEP key settings.

Wired network attacks

Once an intruder has associate with an AP he has access to the network in the same fashion as connecting to the Ethernet cable.

Diagram



For virtually all of the exploits in this discussion the connection diagram is essentially as above. The intruder connects to an access point via a radio connection.

The connection distance is typically 10 to 100 meters inside a building but with directional antennas an added gain at 2.4 Gigahertz can allow connections up to 1000 feet from an AP. This makes this exploit particularly threatening.

How to use the exploit

Direct sniffing – WEP off

Simply deploying a commercial sniffer such as AiroPeek will accomplish this.

Traffic analysis – WEP on

Simply deploying a commercial sniffer such as AiroPeek will accomplish this.

Decryption of encrypted packets – WEP on

To accomplish this it is necessary to have a mechanism for intercepting and recording packets, a commercial sniffer will accomplish this. Additionally a simple program for performing exclusive-or operations is needed.

AP hijacking

Associate with the AP and scan for port 80 responses looking through an IP range used on the network.

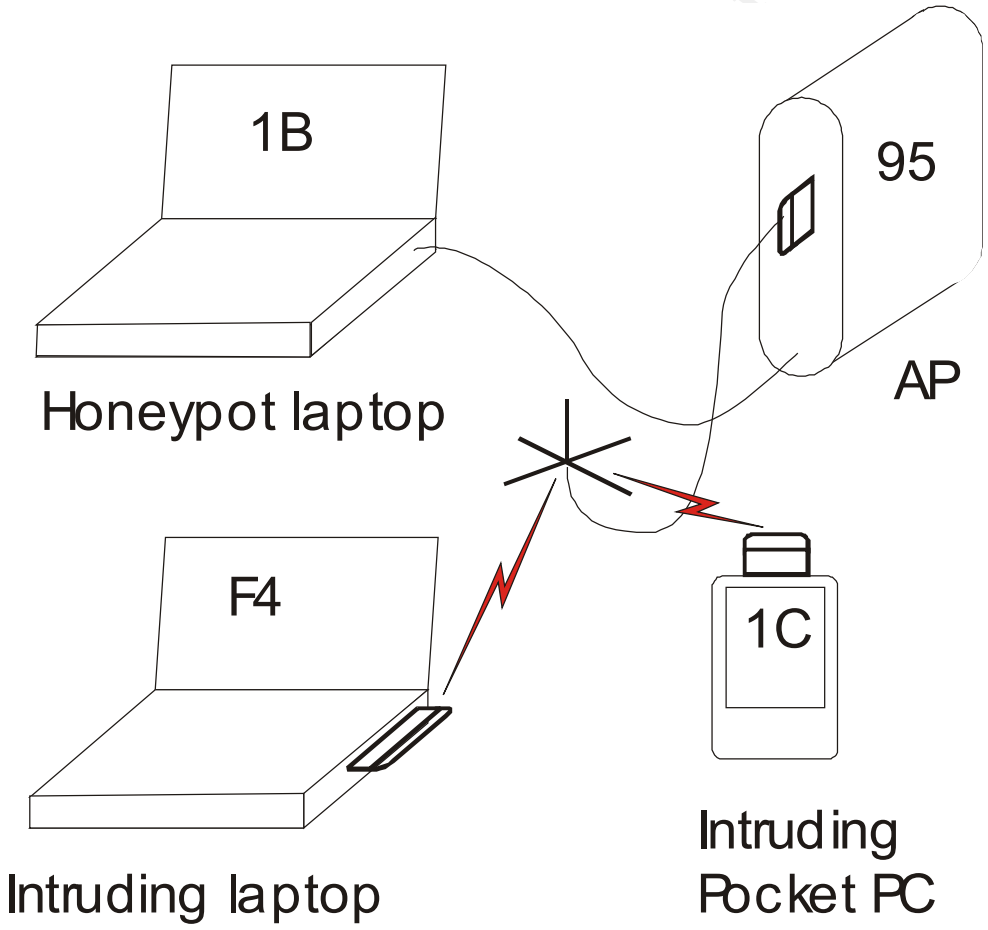
Wired network attacks

Associate with an AP, conduct any desired network attack.

Signature of the attack

This section assumes the honeypot configuration illustrated below. Other configurations can be used while system setup is being completed if an attentive operator is present. The design of this honeypot assumes that monitoring for weeks or months are necessary to catch intruders. Continuous monitoring, possibly via SNMP, is the long term solution to the need for a prompt alert of intrusion.

If SNMP monitoring is used it can be implemented by defining an empty Access Control List in an AP setup. Any intruder who attempts to associate with the AP will create a reportable event which can be trapped. This will alert system operators to the attack allowing other APs configured as honeypots to be examined. If the intrusion response is prompt the person who is attempting entry may be caught.



Here a laptop running conventional sniffer software, in this case CommView[11]. The laptop and AP are connected with an Ethernet cable and the AP is connected to a 2.4 Gigahertz antenna. The antenna used in this case is a simple vertical quarter wavelength

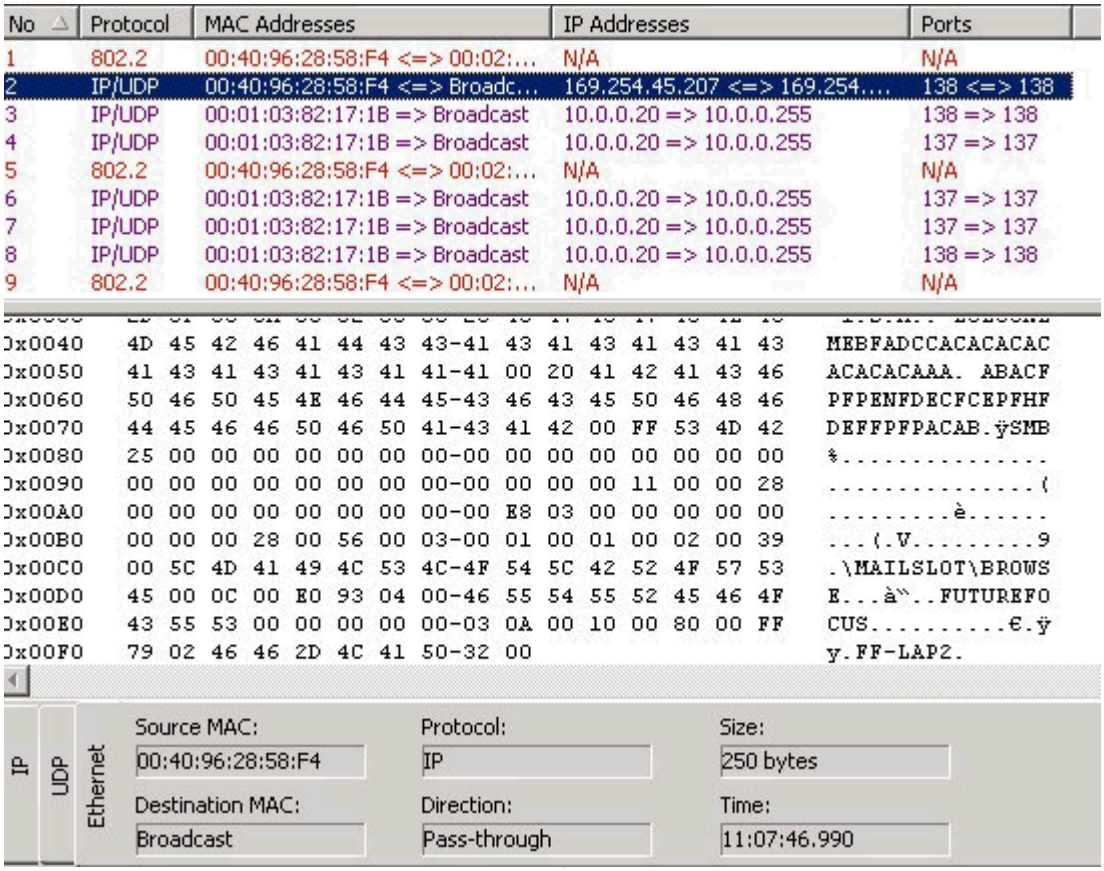
(2 inch long) element with quarter wave radials.

It is important to note the numbers on each component. They represent the last 2 hex digits of the MAC for that component and will be important in the sniffer screen captures later in this section. For example, the MAC address of the Ethernet card in the honeypot laptop is 00:01:03:82:17:1B.

The whole honeypot setup is shown in the following photo.

Intrusions are very simple to observe. The domain is given an ESSID that separates it from other legitimate traffic but is attractive to intruders. In this case the assigned ESSID was "ExecutiveDomain". Since the only traffic observed on the Ethernet is related to the laptop, e.g., NetBIOS, all other events represent intrusions.

Examples are shown in the following screen captures from CommView.



No	Protocol	MAC Addresses	IP Addresses	Ports
1	802.2	00:40:96:28:58:F4 <=> 00:02:...	N/A	N/A
2	IP/UDP	00:40:96:28:58:F4 <=> Broadc...	169.254.45.207 <=> 169.254....	138 <=> 138
3	IP/UDP	00:01:03:82:17:1B => Broadcast	10.0.0.20 => 10.0.0.255	138 => 138
4	IP/UDP	00:01:03:82:17:1B => Broadcast	10.0.0.20 => 10.0.0.255	137 => 137
5	802.2	00:40:96:28:58:F4 <=> 00:02:...	N/A	N/A
6	IP/UDP	00:01:03:82:17:1B => Broadcast	10.0.0.20 => 10.0.0.255	137 => 137
7	IP/UDP	00:01:03:82:17:1B => Broadcast	10.0.0.20 => 10.0.0.255	137 => 137
8	IP/UDP	00:01:03:82:17:1B => Broadcast	10.0.0.20 => 10.0.0.255	138 => 138
9	802.2	00:40:96:28:58:F4 <=> 00:02:...	N/A	N/A

```
0x0040   4D 45 42 46 41 44 43 43-41 43 41 43 41 43 41 43   MEBFADCCACACACAC
0x0050   41 43 41 43 41 43 41 41-41 00 20 41 42 41 43 46   ACACACAAA. ABACF
0x0060   50 46 50 45 4E 46 44 45-43 46 43 45 50 46 48 46   PFPENFDECFCEPFHF
0x0070   44 45 46 46 50 46 50 41-43 41 42 00 FF 53 4D 42   DEFFPFPACAB.ÿSMB
0x0080   25 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00   %...............
0x0090   00 00 00 00 00 00 00 00-00 00 00 00 11 00 00 28   ...............(
0x00A0   00 00 00 00 00 00 00 00-00 E8 03 00 00 00 00 00   .........è......
0x00B0   00 00 00 28 00 56 00 03-00 01 00 01 00 02 00 39   ...(.V.........9
0x00C0   00 5C 4D 41 49 4C 53 4C-4F 54 5C 42 52 4F 57 53   .\MAILSLOT\BROWS
0x00D0   45 00 0C 00 E0 93 04 00-46 55 54 55 52 45 46 4F   E...à“..FUTUREFO
0x00E0   43 55 53 00 00 00 00 00-03 0A 00 10 00 80 00 FF   CUS...........€.ÿ
0x00F0   79 02 46 46 2D 4C 41 50-32 00                     y.FF-LAP2.
```

IP | UDP | Ethernet

Source MAC:	Protocol:	Size:
00:40:96:28:58:F4	IP	250 bytes
Destination MAC:	**Direction:**	**Time:**
Broadcast	Pass-through	11:07:46.990

Here normal traffic from the honeypot laptop (MAC ending in 1B) is seen with an intruding laptop (MAC ending in F4). One of the intruding packets is illustrated; it comes from a computer which is set up on the FUTUREFOCUS workgroup and has a name FF-LAP2.

The honeypot has caught this intruder but the best part is that the machine is also identified via the MAC address as well as networking information. Capturing and recording this information is crucial to intrusion handling. It provides intelligence on the problem as well as a record which may be valuable in prosecution of intruders.

No	Protocol	MAC Addresses	IP Addresses	Ports
268	IP/UDP	00:01:03:82:17:1B => Broadcast	10.0.0.20 => 10.0.0.255	137 => 137
269	IP/UDP	00:01:03:82:17:1B => Broadcast	10.0.0.20 => 10.0.0.255	137 => 137
270	IP/UDP	00:01:03:82:17:1B => Broadcast	10.0.0.20 => 10.0.0.255	138 => 138
271	IP/UDP	00:01:03:82:17:1B => Broadcast	10.0.0.20 => 10.0.0.255	137 => 137
272	IP/UDP	00:01:03:82:17:1B => Broadcast	10.0.0.20 => 10.0.0.255	137 => 137
273	IP/UDP	00:01:03:82:17:1B => Broadcast	10.0.0.20 => 10.0.0.255	137 => 137
274	IP/UDP	00:01:03:82:17:1B => Broadcast	10.0.0.20 => 10.0.0.255	138 => 138
275	IP/UDP	00:01:03:82:17:1B => Broadcast	10.0.0.20 => 10.0.0.255	137 => 137
276	IP/UDP	00:01:03:82:17:1B => Broadcast	10.0.0.20 => 10.0.0.255	137 => 137
277	IP/UDP	00:01:03:82:17:1B => Broadcast	10.0.0.20 => 10.0.0.255	137 => 137
278	IP/UDP	00:40:96:47:54:1C <=> Broad...	0.0.0.0 <=> 255.255.255.255	68 <=> 67
279	IP/UDP	00:40:96:47:54:1C <=> Broad...	0.0.0.0 <=> 255.255.255.255	68 <=> 67
280	IP/UDP	00:40:96:47:54:1C <=> Broad...	0.0.0.0 <=> 255.255.255.255	68 <=> 67
281	802.2	00:40:96:47:54:1C <=> 00:02:...	N/A	N/A
282	IP/UDP	00:40:96:47:54:1C <=> Broad...	0.0.0.0 <=> 255.255.255.255	68 <=> 67
283	802.2	00:40:96:47:54:1C <=> 00:02:...	N/A	N/A
284	IP/UDP	00:40:96:47:54:1C <=> Broad...	0.0.0.0 <=> 255.255.255.255	68 <=> 67
285	IP/UDP	00:40:96:47:54:1C <=> Broad...	0.0.0.0 <=> 255.255.255.255	68 <=> 67

This screen capture of the Ethernet sniffer on the honeypot computer shows normal activity in lines through 277. The red lines, 278 and subsequent are an intruding Pocket PC which is attempting to associate with the AP. Inside this Pocket PC the ESSID has been set to null allowing it to associate with any AP regardless of the AP ESSID setting.

This security weakness can be demonstrated by (an authorized, of course) wireless computer wandering through an airport or downtown area associating with dozens of APs. Often this simple association technique allows direct connection to the Internet demonstrating the vulnerability to the most basic intrusion techniques.

The popular "drive by" association with networks[12] uses this technique but it can be easily recognized by the honeypot described in this document.

How to protect against it

The 802.11 standard should be changed to

- Increase the length of the IV
- Remove authentication challenge problems.

Network PC card vendors should

- make certain that all frames roll IVs
- protect secret keys from discovery outside of the card

Network users should

- Always use IPsec, ssl, ssh,… to encrypt all traffic over the wireless network
- Require WEP for all wireless connections
- Disable AP setup via radio
- Recover PC cards with WEP keys from departing employees to prevent their using them for unauthorized access
- Deploy only current AP firmware
- Use MAC Access Control Lists ACLs where possible
- Install an AP with an ACL having no entries to detect intruders via SNMP traps
- **Install a honeypot as described in this document to document intrusions**

Source code/ Pseudo code

Since this exploit and its defenses use application-level tools, a source code discussion is not applicable.

Additional Information

The following references are useful in understanding wireless systems and their flaws. Unless a detailed study is necessary it is not necessary to purchase the standard. The best quick study on the topic is O'Hara/Petrick.

[1] G. Mitchell, Wireless LANs - the Big New Security Risk, May 5, 2000
http://www.sans.org/infosecFAQ/wireless/LAN.htm

[2] All photos in this paper are courtesy of Future Focus, Inc http://www.bug-killer.com/

[3] Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium AccessControl (MAC) and Physical Layer(PHY) Specifications International Standard ISO/IEC 8802-11: 1999(E) ANSI/IEEE Std 802.11, 1999 Edition available from http://standards.ieee.org/

[4] AiroPeek (a commercial wireless sniffer) and EtherPeek (an Ethernet sniffer) are available from http://www.wildpackets.com/

[5] Bob O'Hara, Al Petrick, **802.11 Handbook: A designer's companion,** IEEE Press, NY, NY, 1999

[6] RC4 was developed by Ron Rivest of MIT (and later RSA Data Systems) it is a stream cipher which is very efficient in terms of required computer power.

[7] From IEEE Standard 802.11 section 8, Authentication and privacy

[8] IEEE Standard, paragraph 8.1.2, Shared Key authentication

[9] A description of probs with WEP insecurity, solutions include separating encryption from authentication is included in
http://www.zdnet.com/eweek/stories/general/0,11011,2684262,00.html

[10] University of Maryland team finds flaws in wireless protocols
http://www.zdnet.com/eweek/stories/general/0,11011,2704419,00.html
A University of California Berkeley paper on 802.11 weaknesses
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[11] Commview is a commercial Ethernet sniffer available from http:/www.tamosoft.com

[12] Drive-by association with networks has been publicized in the popular press. See

http://www.msnbc.com/news/565275.asp?cp1=1