Introduction to Wireless Auditing

Sean Whalen
January 2002

PURPOSE

The goal of this paper is to demonstrate how to perform a simple audit of a wireless network employing the 802.11b protocol.

Many papers have been published on the weaknesses of the 802.11b protocol[1] and the Wired Equivalency Protocol (WEP)[2]. Instead, I aim to show the reader how to test and improve the security of a wireless network. I will take a high level approach to these problems, with detailed video and resources available through my website located at http://chocobospore.org.

THE BASIC PROBLEM

The world of wireless networking has exploded in the past two years, with the market growing from $600 million in 1999 to over $1.6 billion at the end of 2001[3]. This growth has been driven by the advent of affordable devices implementing the 802.11b wireless networking protocol, an extension to the 802.11 wireless specification, originally ratified in 1997 by the IEEE. The main advantage of 802.11b for most users is a comparable data rate standard Ethernet: 11 megabits per second, versus 2 megabits for the original 802.11.

Security was also a concern when designing 802.11b. Encryption is supported in the form of the Wired Equivalency Protocol (WEP). Unfortunately, the protocol is inherently flawed in several regards which we will explore later. WEP provides only the illusion of security.

The bottom line is very simple: when you use wireless technology, your information is going through the air. Anyone can transmit, and anyone can receive.

[1] http://www.cs.umd.edu/~waa/wireless.html
[2] http://www.cs.rice.edu/~astubble/wep/wep_attack.html
[3] http://www.forbes.com/2001/12/10/1210sf.html

There is no wire to guide your signal. With the explosion of 802.11b, we have seen the first wide-scale deployment of wireless networking. There is more information being transmitted and many more people capable of receiving it. Because the underlying protocol is insecure, the information relayed is insecure. In addition, WEP offers little to no protection, creating a false blanket of security for many business and home users.

CONNECTIVITY

There are several 802.11b topics which need to be well understood in order to perform an audit. This paper does not aim to be a tutorial on the protocol, but we will cover connectivity basics as they are essential to the task of auditing.

There are two basic modes of communication for 802.11b networks: ad-hoc and infrastructure. Ad-hoc mode allows devices to communicate as long as they are within range of each other. This range is defined by transmit power, antenna size and type, distance, geography, obstructions, and weather.

Infrastructure mode relies on an access point, also called a base station, to act as a central point of communication. Mobile devices must associate (request and be granted access) to the access point, at which time they can communicate with any other associated devices. Many popular access points are also Ethernet bridges or routers, providing wireless devices access to wired networks and/or the internet. With regards to auditing, we are concerned with infrastructure mode.

Both modes rely on ‘beacons’ to discover other mobile devices. A beacon is one of many special wireless frames which perform the low level duties of 802.11b. The most important information a beacon contains is a network name, or ‘SSID’. When a device transmits a beacon frame, which can occur several times per second, it is advertising itself to the world in hopes of finding something else to communicate with. When a device receives a beacon frame, it has all the information it needs to communicate with the transmitting device; namely, the SSID.

The insecurity of 802.11b lies within the use of the SSID as the authentication mechanism. Typically, the only information needed to associate with an access point is the SSID of the device. Since access points will be broadcasting their SSID to the world several times per second, the only thing needed to access these networks is the ability to grab the SSID from beacon frames. Even with WEP turned on, the network still broadcasts beacons in the clear. This becomes incredibly frightening if your access point is also a bridge, giving any associated wireless devices access to your internal wired network.

AUDITING

To defend your network against intruders, you must employ their methods. The most commonly used methods of breaking into wireless networks are very simple, as are the defenses. We will be focusing on these common methods used by the casual would-be intruder, usually termed war drivers or war walkers[4].

War drivers and walkers are people equipped with laptops or handhelds, wireless cards, usually an antenna, and special software. Walkers will be on foot, while drivers use a vehicle primarily as a means of detecting networks over a large area. Driving provides a reduced risk of being noticed as well.

Before auditing, it is important to understand the capabilities and goals of a typical attacker. An attacker is usually interested in gaining access to the wired segment of a network, either to collect information or to bring the network down. This is made particularly easy if the wireless access point also provides an unprotected bridge to a wired segment.

[4] http://www.wardriving.com

Attacks such as ARP spoofing are equally effective over both wired and wireless links[5]. A wireless attacker who gains access to a bridged segment is virtually sitting at a terminal on your internal network, with the added bonus of a quick and easy escape. When possible, separating your wireless segment from your wired segment will go a long way towards preventing disaster.

In addition, be wary of sensitive information being sent in the clear by wireless clients as this information could provide an attacker with all they need to access resources through other means. Usernames and passwords are ripe for the picking if they are transmitted within the range of an attacker. In this case, WEP is indeed better than no WEP for most users. Virtual Private Networks can provide proper protection for those needing true security.

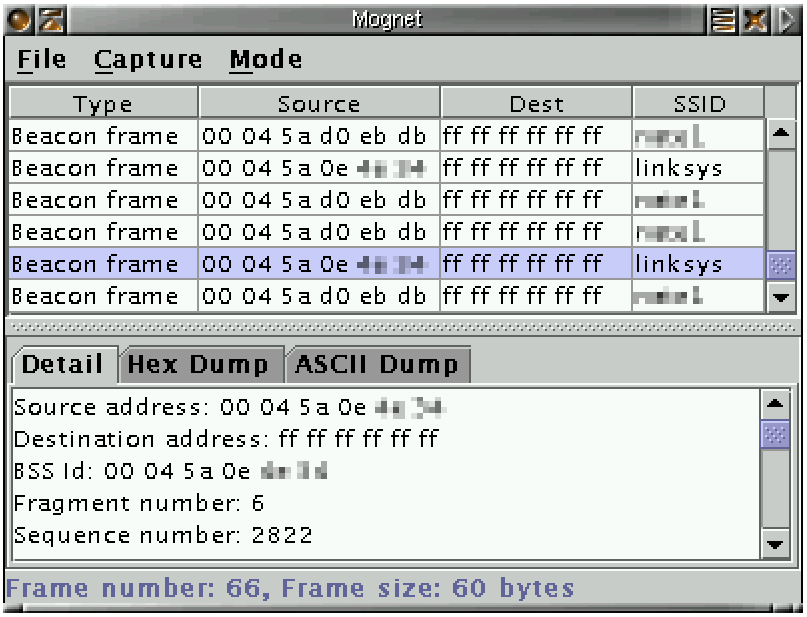
To begin auditing, you will need the same things as the attacker: a laptop or handheld device, an 802.11b network card, a yagi or omni directional antenna, and the right software. The total hardware investment can be less than a thousand dollars[6].

There are only two free 802.11b analyzers available. The first is the well-known Ethereal[7], which has supported 802.11b frames for several months. The second is a Java program I have written called Mognet[8], which is aimed at portable devices and has been successfully tested on iPaq handhelds. There are other programs such as NetStumbler[9] which are not 802.11b analyzers but produce enough information to gain access.

If using a full 802.11b analyzer, you will be able to examine every detail contained in a wireless frame. This includes source and destination MAC addresses, features enabled on the client, features enabled on the access point, supported transmit speeds, current transmit channel, encryption status, SSID, beacon interval, and more. In addition,

[5] http://www.cigitallabs.com/resources/papers/download/arppoison.pdf
[6] http://www.bitshift.org/wardriving.shtml
[7] http://www.ethereal.com
[8] Developed with equipment from the Ubiquitous Computing Lab at the University of Nebraska at Omaha
[9] http://www.netstumbler.com/

you can examine the data portion of the frame, seeing passwords and other data in the clear if WEP is disabled. A screenshot from Mognet is included below to demonstrate:



Type	Source	Dest	SSID
Beacon frame	00 04 5a d0 eb db	ff ff ff ff ff ff	[redacted]
Beacon frame	00 04 5a 0e [redacted]	ff ff ff ff ff ff	linksys
Beacon frame	00 04 5a d0 eb db	ff ff ff ff ff ff	[redacted]
Beacon frame	00 04 5a d0 eb db	ff ff ff ff ff ff	[redacted]
Beacon frame	00 04 5a 0e [redacted]	ff ff ff ff ff ff	linksys
Beacon frame	00 04 5a d0 eb db	ff ff ff ff ff ff	[redacted]

```
Source address: 00 04 5a 0e [redacted]
Destination address: ff ff ff ff ff ff
BSS Id: 00 04 5a 0e [redacted]
Fragment number: 6
Sequence number: 2822
```

Frame number: 66, Frame size: 60 bytes

To begin, you should determine the perimeter of your network. It may surprise you how far your signal propagates. 802.11b is designed to scale well with distance, dropping in speed as signal strength wanes but still providing service down to 1 mb/sec. Although optional, it is important to use a high-gain antenna as most intruders will have one.

After you know where to look for your signal, you should step through the defenses listed in the next section, see which ones you are able to apply, and re-audit. If you can't break in to your own network, it is likely that the casual attacker will also have difficulty and pass you over for an easier target.

Frequent audits are also important. This is best illustrated by the example of a large networking company who encouraged employees to use employee discounts towards access points for home. Many employees brought the access points to work. Visitors touring the facility with laptops noticed they were authenticating to the rogue access points, with full access to the company intranet.

Our goal is not complete security, but rather adequate deterrence. With that in mind, there are several actions you can take to reduce the visibility of your network to intruders, as well as make access more difficult to obtain. Some of these solutions require vendor-specific hardware, or may not be possible for certain network configurations.

- Disable beacon frames on the access point. If this is not an explicit option, try setting the beacon interval to 0. Beacons are sometimes useful, but most networks don't require their use. Some vendors support beacons with an encrypted SSID although this requires compatible clients as well.
- Enable WEP. It's insecure, but despite the anti-WEP hype it is better than nothing. For most networks, it takes a long time to collect the amount of data needed to crack WEP. So few people use it, that merely enabling it will likely deter most prospective intruders. Both 40-bit and 104-bit keys are susceptible to dictionary attacks if a weak passphrase is used, so keep that in mind when generating keys.
- Use a directional antenna. A directional antenna will focus the network transmissions to a specific area, both increasing link strength in that area and decreasing the area for possible intrusion.
- Lower your transmit power. Like above, don't provide coverage where it's not needed.
- Disable DHCP for wireless clients. This will work better if a non-default IP range is used on the network so the attacker can't simply guess which subnet your network uses and assign themselves an IP. Binding MAC addresses to DHCP

leases should not be considered a solution, as changing a device's MAC address is extremely simple.

- Use a vendor-specific solution to provide a secure authentication mechanism, such as RADIUS or LEAP.
- Don't use default SSIDs or passwords on access points.
- Use application-level encryption. Use virtual private networks to encrypt data before it is broadcast as a wireless frame so at least your data isn't vulnerable.

The more of these techniques you can use, the better off you will be. The easiest combination would be removal of beacons, enabling WEP, and adjusting transmit power/antenna type. To truly secure your data, a VPN is essential, although it will not solve the problem of unauthorized access.

WRAPPING UP

Performing a basic audit is very simple: survey the area affected, make changes, and re-survey. If you can't detect the network, intruders likely won't either. If you use a properly implemented VPN, your data is safe even if they are capturing your wireless frames. Repeated audits will ensure the detection of rogue access points or other changes to the network before they become a problem. These simple steps will reasonably protect a small to mid-sized wireless network from the threat of the casual intruder.