Wireless Attacks and Defense

By: Dan Schade

April 9, 2006

As more and more home and business users adapt wireless technologies because of their ease of use and affordability, these devices are coming under attack by the malicious who are after your data and by the casual user looking for free bandwidth. In this paper, I will explain how wireless attacks are done on Wired Equivalency Privacy (WEP) networks, other common network attacks and then present several options to defend wireless networks.

History of 802.11 Wireless Security

Since the summer of 2001, WEP cracking has been a trivial but time consuming process. “Scott Fluhrer, Itsik Mantin, and Adi Shamir identified a key scheduling attack, known as FMS attack, against theRC4 algorithm that, when used with certain keys, renders the cipher vulnerable to key recovery.” (Branch)

A few tools that implement the Fluhrer-Mantin-Shamir (FMS) attack were released to the security community -- who until then were aware of the problems with WEP but did not have practical penetration testing tools. Although simple to use, these tools required a very large number of packets to be gathered before being able to crack a WEP key.

On August 8th, 2004, a hacker named KoreK posted new WEP statistical cryptanalysis attack code to the NetStumbler forums. While it is still functional, it is not currently maintained, and the attacks have since seen better implementations in Aircrack and WepLab just to name a few. The KoreK attacks changed everything. No longer were millions of packets required to crack a WEP key. With the new attacks, the critical

ingredient is the total number of unique IVs captured, and a key can often be cracked with hundreds of thousands of packets, rather than millions.

So even though there is widespread deployment of wireless, why does it attract so much criticism? Arbaugh stated it best when he said “First, there was the exponential adoption rate of the technology. Further, the security architecture did not define a threat model or security goals and was developed by a relatively closed standards body without public review or involvement of a security professional.” (Arbaugh).

Probing and Network Discovery

Transmitting data through the air makes them susceptible to being captured and read by anyone with a receiver capable of listening in on the same frequency that the data is being transmitted.

Wi-fi signals are easy to intercept and WEP security is fairly simple to crack given the right tools. Unfortunately, these tools are readily available and can be downloaded from numerous sites. WPA can be cracked using a brute force dictionary attack if the user uses a simple word or phrase as his key. Simply creating a 20+ word pass phrase interspersed with number or symbols will secure your network (at least for today).

To demonstrate how easy it is for someone to break a WEP code, I did some research on the internet and downloaded a Linux Live CD. After playing with the software to become familiar with it for an hour or two, I was able to crack a WEP secured network in approx 40 minutes.

For hardware I used a Hawkins Technology PCI wireless G card in my desktop. All of the software I used came from the User Edition of the Linux Live CD Backtrack

beta version 05022006 (http://www.remote-exploit.org/index.php/BackTrack_Downloads).

The first step in any attack is to gain information about the network that you want to access. I used the Airodump software to get a feel for what I had to work with. Using the command "**airodump ra0 out 0**" yielded the result seen in Figure 1.

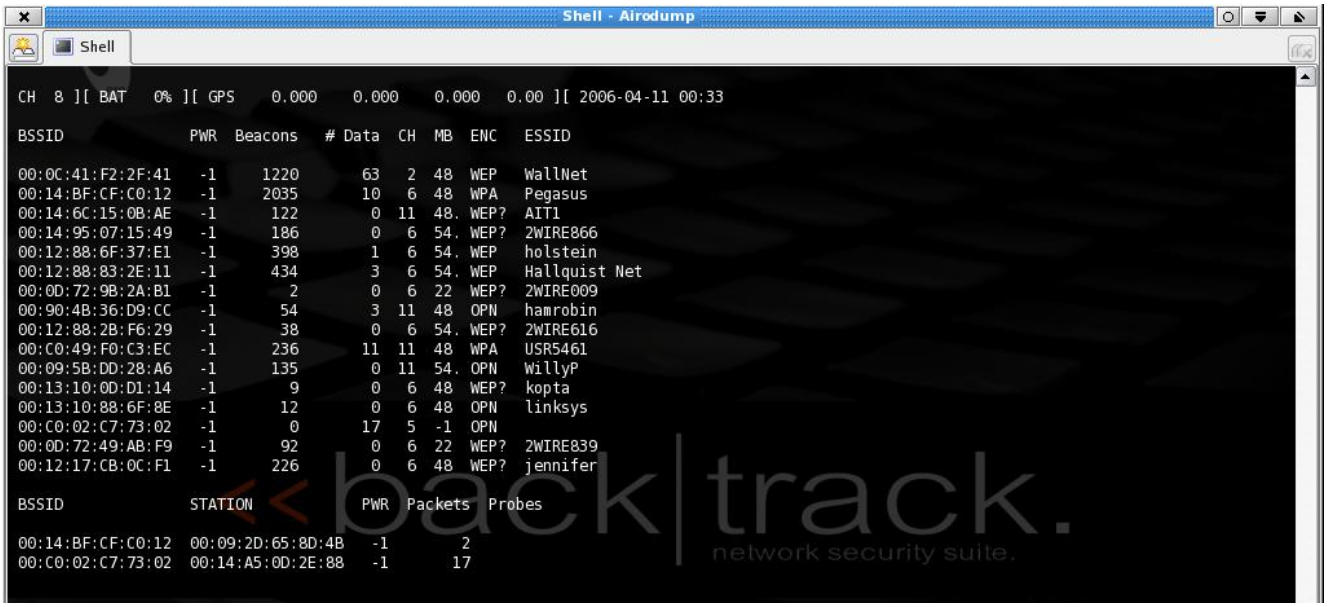

Figure 1 – Airodump Results

As seen in Figure 1, I was able to pick up some level of signal from 16 networks. The ENC column shows the encryption for the various networks.

I created a Pareto analysis of the data in Chart 1 which shows that 14.3% of the networks used WPA, 64.3% used WEP and the remaining 21% were completely open.

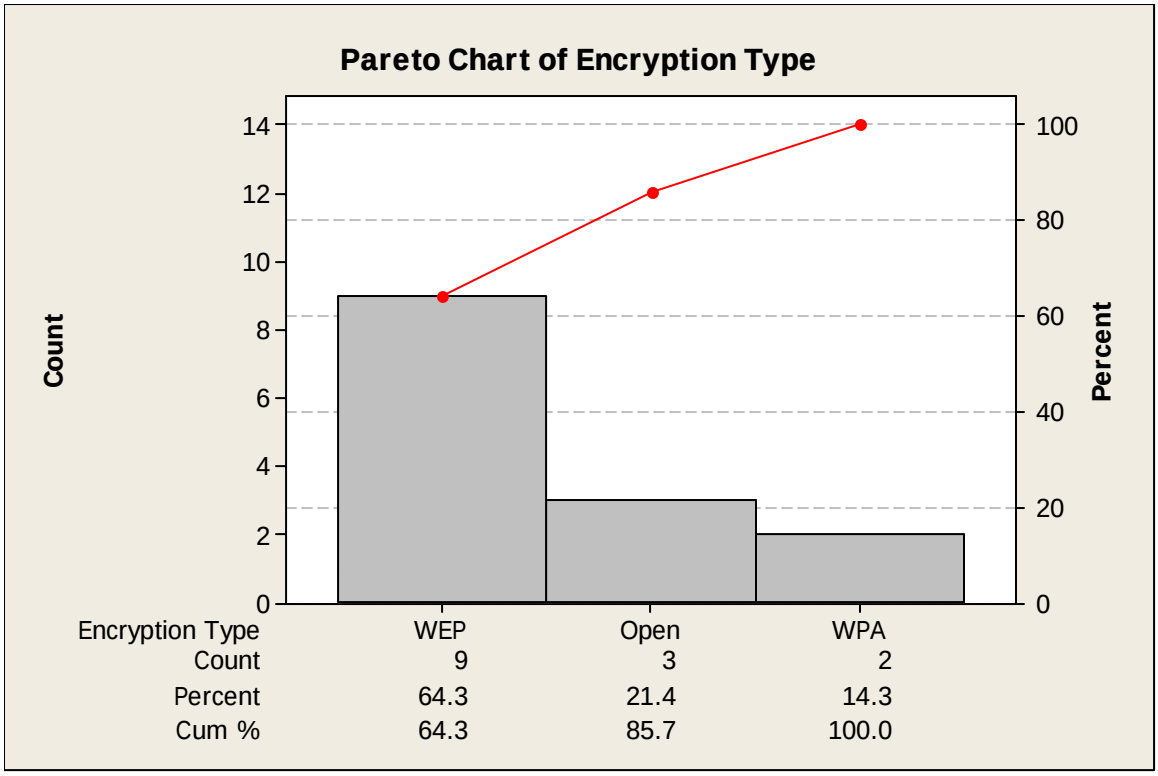

Chart 1 – Pareto Analysis of Encryption Types

The Pegasus network, my network, was configured as WPA when I ran the scan, but after running the scan, I changed it to WEP so that I could run the attack on my own network rather than intruding on my neighbors.

Airodump also gives you some other useful information and we will take note of it. The BSSID is the MAC address of the Access Point (AP) which we will need later on in our attack. Down towards the bottom there is a subsection that shows active user MAC addresses on the networks. This could be important if we find that the AP is using MAC filtering and have to spoof them.

Surveillance

After changing my router to 128-bit WEP and creating a key composed of random characters, I issued the following command, "**airodump ra0 out 6"** to capture traffic from available networks that were on channel six. This just helps keep your file size to a minimum and you could leave it to option 0, all channels if you were so inclined.

Since I had very little traffic on my network, most of it is hard wired, it would have taken a long time to capture enough data to successfully figure out what the key is using Aircrack. In Humphrey's article the feds stated that, "the number of packets required for success with Aircrack varies greatly. As a rule of thumb, shoot for a minimum of 200,000 for a 64 bit key and 500,000 for a 128 bit key." (Humphrey) The packets to look for are called WEP Initialization Vectors (IV). So I dipped into the bag of tricks provided with the Backtrack distribution. This time I pull out Aireplay. This piece of software will inject data into the network which forces the AP to respond with encrypted packets.

First you have to authenticate to the IP as seen below in Figure 2:

```
# aireplay -1 0 -e Pegasus -a 00:14:BF:CF:C0:12 -h 0:1:2:3:4:5 ra0
11:14:06  Sending Authentication Request
11:14:06  Authentication successful
11:14:06  Sending Association Request
11:14:07  Association successful :-)
```

Figure 2 – Aireplay Authentication

If MAC addressing filter is being used, you will not be able to authenticate to the AP using the bogus MAC ID of '0:1:2:3:4:5' that I used, but instead would have to monitor the network and capture a station MAC address and use that in lieu of the bogus MAC address. Not a huge hurdle to overcome, but this still helps you keep the casual wardriver off of your network.

Once associated, you can use Aireplay to inject packets. Figure 3 shows what it looks like.

```
root@slax:~# aireplay -3 -b 00:14:BF:CF:C0:12 -h 0:1:2:3:4:5 -x 800 ra0
Saving ARP requests in replay_arp-0411-110017.cap
You must also start airodump to capture replies.
Read 1148795 packets (got 552781 ARP requests), sent 599232 packets...
```

Figure 3 – Aireplay Packet Injection

I let my system capture information for approximately 40 minutes. This was probably overkill on my part as you don't need as many IVs as I collected. In the 40 minute time I was injecting and capturing packets, I captured 1.4 million IVs.

Next, I pulled out my last trick, the application Aircrack. Using the command "aircrack -x -0 out-02.cap" I received the results shown in Figure 4 after the program ran for 10 seconds. You can actually run Aircrack at the same time you are capturing packets, but I did them separately.

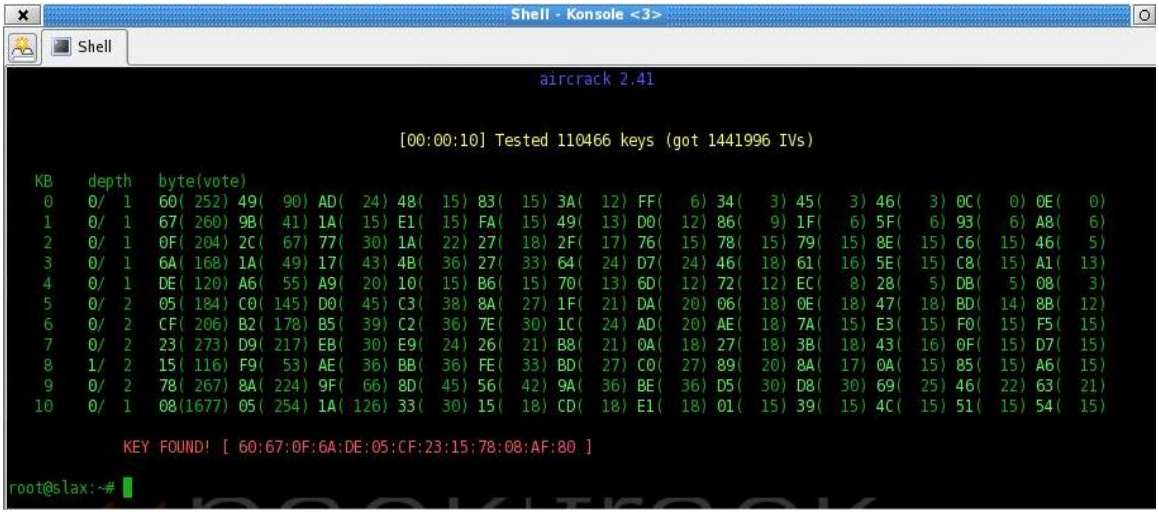

Figure 4 – Key Found!

Once you have the key, you can authenticate either manually in Linux or using the wireless connection wizard in Windows.

So a little bit of research, some free software, and a couple of hours of time and I was ready and able to crack a WEP secured network. You can use some of the same tools to attempt to find a WPA passphrase because it is not immune to being cracked, but all the tools out there currently require the use of a dictionary attack. Randomizing your pass phrase will significantly reduce the risks that your WPA network can be successfully cracked. Open networks or even WEP encrypted networks are much easier to gain access to. Using the tools contained on the Backtrack distribution and some time we could access fourteen of the sixteen networks within range of my wireless card fairly easily.

Your best defense is to upgrade to WPA or WPA2 which uses AES. Just about all 802.11g routers, and some 802.11b, can be upgraded to support WPA by merely updating their firmware. Only two of the wireless networks that I picked up from my house were 802.11b so more than likely, all of these could have been upgraded at no cost to the user. For those that are stuck using WEP, it is still better than nothing. To defeat the casual wardriver, just having WEP is good because as we saw in my case, some people leave their networks wide open. So, enable WEP with a 128-bit key. Change the key every month or 90 days. Enabling MAC filtering is another step you can take, although it is easy to defeat. The next best thing you can do is to just shut it off when you are not using it. You can buy a cheap lamp timer from the store for $5 or so and set it to turn off every night. You can't be hacked if there is no signal.

Denial of Service (DoS) Attacks

Denial of service attacks can take place at the physical, data-link and network layer of the OSI model. For the physical layer, "An adversary can simply disregard the medium access protocol and continually transmit on a wireless channel. By doing so, he

either prevents users from being able to commence with legitimate MAC operations, or introduces packet collisions that force repeated backoffs, or even jams transmissions." (Xu) For people using 2.4Ghz routers, they are warned not to use cordless phones operating on the same frequency because the phone can cause interference on the router and vice versa. "Unfortunately, many 2.4 GHz cordless phones that can be purchased in electronics stores have the capability to take an 802.11b network offline. While not a refined electronic weapon, these phones can interfere or completely disable a WLAN." (Anonymous). More elaborate forms would include creating a radio or using an amplifier that outputs significantly more wattage than a telephone transmitter and could effectively shut down a wireless network.

Attacks on layer 2 can target either a host or network. Data link attacks disable the ability of hosts to access the local network. Most data link attacks are typically in the form of packet injection. In this type of attack the attacker will flood wireless clients who are already attached to the network with disassociate or de-authenticate packets. There are several tools available to send out de-authentication packets to include one called Void 11.

A network layer DoS is accomplished my sending copious amounts of data to a network and attempts to overwhelm the capacity of the network. For example, if you are running a 10Mb/s network, an attacker could use multiple computers and send 100Mb/s of data. Since the network is not designed to carry this much traffic it will be forced to drop packets, both from legitimate users and from the attacker. The excessive traffic will also serve to cause a high load on the processors of the wireless access points. An

example of such an attack would be for an attacker to send an ICMP flood (ping) to the gateway.

Impersonation

Impersonation attacks in a wireless network typically involve an attacker taking on the address of a valid client or AP and trying to obtain access or services typically reserved for those valid clients or APs. In a worst-case scenario, an impersonating AP could fool a client into connecting with it, and then obtain that client's authentication credentials.

A defense against impersonation for wireless clients that have been authenticated and associated is by using software that monitors the sequence number field within the IEEE 802.11 header. Usually when impersonation attacks are underway, the attacker will take on the MAC / IP address of the victim, but it will not be able to continue with the sequence number used previously by the victim, thus by monitoring the sequence number in these client generated packets, impersonators could potentially be identified.

For business users, WPA/WPA2 deployment and encryption at higher levels in the protocol stack are necessary for critical applications. Business users should also deploy network sniffers in conjunction with an intrusion detection system which looks for various types of attacks to include the ones mentioned in this paper and have processes in place to deal with the attacks.

In conclusion, wireless technologies have continued to evolve to the point that they are common place. These networks are susceptible to various types of attacks merely because they are transmitted through the air and cannot be physically secured. WEP attacks are easy to defeat by merely upgrading firmware in your router and using a

strong pass phrase, although many users don’t have the knowledge or desire to take these easy steps.

Works Cited

*Branch, Joel W. "Autonomic 802.11 Wireless LAN Security Auditing." IEEE Security & Privacy. May/June 2004: 56-65.

*Arbaugh, William. "Wireless Security is Different." Computer. Volume 36, Issue 8, Aug. 2003: 99–101.

Humphrey, Cheaung. "The Feds can own your WLAN too" Tom's Networking . 3 April 2006. <http://www.tomsnetworking.com/2005/03/31/the_feds_can_own_your_wlan_too/>.

*Xu, Wenyuan. "The Feasibility of Launching and Detecting JammingAttacks in Wireless Networks" 4 April 2006. <http://www.winlab.rutgers.edu/~trappe/Papers/JamDetect_Mobihoc.pdf>

Anonymous. "802.11 Wireless Networks Risk Assessment Form" 3 April 2006. <http://www2.state.id.us/ITRMC/plan&policies/guidelines/g530.htm#Appendix_C>