Fourth LACCEI International Latin American and Caribbean Conference on Engineering and Technology (LACCEI '2006) "Breaking Frontiers and Barriers in Engineering: Education, Research and Practice", 21-23 June 2006, Mayaguez, Puerto Rico

Security Threats in Wireless Networks

Alvaro E. Escobar, PhD ABD
PhD Candidate, Department of Computer Science and Engineering
Florida Atlantic University, Boca Raton FL USA aescoba1@fau.edu

Abstract
Today there are many ways to connect to a network wirelessly, using different devices (laptops, cell phones and Personal Digital Assistants (PDAs)) and through many different wireless protocols. This gives us the privilege to access an immensely amount of information on the World Wide Web and stay in touch with one another conveniently, but it also posses an equally amount of threats to viruses, privacy violations and online scams. In this survey I will identify what are the security threats in a wireless network and describe the countermeasures that a wireless network administrator can take to reduce the risks.

Keywords
Security, Wireless Networks, IEEE 802.11, WEP

1. Introduction

The widespread area of 802.11 network coverage zones is one of the major reasons for rising security concerns and interest. Currently the attackers of wireless networks appear to be more persistent and efficient than the defenders; the reason being new attack tools and methodologies appear on a monthly, if not weekly basis. In this paper I will cover the real world wireless security threats and therefore I have divided it in two major parts; attacks and defense on wireless networks.

2. Real World Wireless Security

In the majority of cases an attacker does not have to do anything to get what he or she wants because the safe door is open and the goods are there to be taken. Wardrive observations and contests concluded that only 27% of wireless networks were protected by WEP (wired equivalent privacy).

As for the future of 802.11 security, it is not as bright as it seems due to several reasons:

- Manufacturers are releasing equipment onto the market even though the standard is not complete.
- Some of the products released in the market are not even security certified.

3. Attackers and their reasons to attack

We can outline six reasons why attackers would want to attack your wireless network:

- It is fun. Many geeks find hacking that involves tweaking both software (sniffing / penetration tools) and hardware (PCMCIA cards, USB adapters, connectors, antennas, amplifiers) more exciting than more traditional cracking over wired links.
- An attacker is difficult to trace. Any time the attacker logs in from his or her ISP account, he or she is within a single `whois` command and a legally authorized phone call from being caught.
- Some might view illicit wireless access as a way of preserving one's online privacy.
- In addition, there are purely technical reasons (apart from the vague network perimeter) that make wireless networks very attractive for crackers.
- A cracker can install a PCMCIA / PCI card / USB adapter / rogue access point as an out-of-band backdoor to the network.
- There is always "opportunistic cracking."

Knowing what kind of individual might launch an attack against your wireless network is just as important as being aware of his or her motivations. From the motivations already outlined, it is possible to split attackers of wireless networks into three main categories:

- Curious individuals who do it for both fun and the technical challenge.
- "Bandwidth snatchers."
- Real Black Hats who happen to like wireless.

4. 802.11 Hardware

The first question that beginners ask before assembling their kit is whether a laptop or a PDA should be used for wireless penetration testing of any kind. The main advantage of PDAs (apart from size) is decreased power consumption, letting you cover a significant territory while surveying the site. The main disadvantage is the limited resources, primarily nonvolatile memory. However, if you want more than just network discovery and packet capture, you will need a UNIX-enabled PDA with a collection of specific tools. A compromise in the "PDA vs. laptop" dilemma would be: Use the PDA running some signal strength monitoring software (e.g., wavemon or Wireless Monitor) for site surveys and rogue access point (or even user) discovery and the laptop loaded with the necessary tools for heavy-duty penetration testing.

PCMCIA and CF Wireless Cards is probably the most important choice when selecting the equipment for your complete kit. The reason lies in the significant differences among the wireless client cards available, including the following:

- *The chipset*: From the wireless security auditor and hacker viewpoint, it is important to have open specifications and open source drivers for these chipsets, allowing the monitor mode, software access point functionality, and ability to build and mangle wireless frames.
- *The output power level and the possibility of its adjustment*: Higher power output means the chance of connecting to the target network from a longer distance, better capability to launch jamming DoS attacks, and increased chances of Layer 1 man-in-the-middle attack success. Better receiving sensitivity means more wireless networks detected when scouting, higher connection speed when associating to the WLAN, and more wireless traffic dumped and analyzed.
- *The receiving sensitivity and amount of external antenna connectors*: From the attacker's perspective, antennas give distance (resulting in physical stealth), better signal quality

(resulting in more data to eavesdrop on and more bandwidth to abuse) and higher power output (essential in Layer 1 DoS and man-in-the-middle attacks). From the defender's perspective, correctly positioned antennas limit the network boundaries and lower the risk of network detection while reducing the space for attackers to maneuver.
- *The support for 802.11i and improved WEP versions*.

5. 802.11 Software and Drivers

The majority of the techniques and methodologies to hack a wireless network are based on open source software because when doing anything related to wireless hacking, you want to operate with "hackable" software you can modify and optimize for your specific needs and hardware at hand. Naturally, Linux comes as the platform of choice for running, tweaking, and developing such software. All drivers use the same `/etc/pcmcia/wireless.opts` configuration file, supplemented by more specific configurations such as `wlan-ng.conf`, `hermes.conf`, `hostap_cs.conf`, or `vt_ar5k.conf`. These additional files contain the description of 802.11 cards known to be supported by a particular driver they come with.

6. WarDrive: Network Mapping, Site Surveying

Wardriving is the term for finding and marking the locations and status of wireless networks. Wardrivers typically use software to determine whether the network is open or closed and a GPS (Global Position System) device to record the location. As long as you don't abuse the found networks' resources and don't eavesdrop on bypassing data traffic, wardriving or warwalking is not illegal. Network discovery tools are the most abundant; the majority of them are free. Some of these tools are more than just network mapping software, and support advanced features such as WEP decryption on the fly or wireless IDS signature database. There are three ways of discovering wireless networks:

- *Active scanning*: Active scanning refers to sending a probe request frame and waiting for probe responses to come back. The received probe response frames are dissected to show the network ESSID (extended service set identifier), channel, the presence of WEP, signal strength, and supported bit rate. Active network discovery is implemented by Netstumbler and Mini-Stumbler, Windows tools most frequently used by casual wardrivers around the world.
- *Monitor-mode sniffing and Traffic Analysis*: The most common and useful group of wireless network discovery and traffic analysis tools use the RFMON mode combined with hopping through all DSSS (Direct Sequence Spread Spectrum) channels. This lets you discover wireless hosts via detecting and analyzing passing traffic including all kinds of control and management frames.
- *Searching for AP (Access Points)*: The main advantage provided by tools under this category is the possibility to discover access points in the area without disconnecting from the network you are already associated with.

7. Tools of the Trade

All wireless penetration testing-specific tools can be split into several broad categories:

- *Encryption cracking tools:* By definition, these tools break 802.11-specific Layer 2 cryptographic protection. This is by no means limited to cracking WEP. Even with the "ultrasecure" AES-based CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) there is always a possibility of dictionary and brute force attacks

and the potential for development of cracking tools to launch these attacks. Currently, there are four classes of wireless encryption cracking tools:

- WEP crackers: With a brute force attack, you only need to capture a single encrypted packet and then apply an enormous amount of computing power. FMS attacks, on the other hand, rely on capturing an enormous amount of encrypted traffic, then using very little CPU power for a probabilistic algorithm to crack the key. Some tools are:
  - AirSnort
  - Wepcrack
  - Dweputils
  - WepAttack
- Tools to retrieve WEP keys stored on the client hosts: These tools recover WEP keys saved in the Windows registry under a crackable encryption and obfuscation. The only such tool available is called LucentRegCrypto utility.
- Traffic injection tools accelerating WEP cracking: To perform this task you will need a card in the RFMON mode, listening to the packets flying by and retransmitting the packets that pass a certain sanity check. Of course, you need to know the ESSID to inject the traffic, so you'll first need to sniff it out. The only such tool available is called Reinj and works by duplicating predictable packets on the WLAN.
- Tools to attack 802.1x authentication systems: At the moment 802.1x authentication using Cisco EAP-LEAP takes the heaviest impact from the hacking community. The reason for this is probably the abundance of EAP-LEAP supporting networks due to the widespread use of Cisco wireless equipment and the fact that LEAP, like older EAP-MD5, relies on password and not certificate-based authentication. Some tools are:
  - Leapcrack
  - Asleap-imp and Leap

- *802.11 frame-generating tools:* Because 802.11 management and control frames are neither authenticated nor encrypted, being able to send custom 802.11 frames gives a wireless attacker an unlimited opportunity to cause Layer 2 DoS (Denial of Service) attacks on a targeted WLAN. Even worse, a skilled attacker can spoof his or her attacking machine as an access point, wireless bridge, or client host on the unfortunate infrastructure or managed network or as a peer on the independent or ad-hoc WLAN. Then a DoS attack can be used to deassociate WLAN hosts from a legitimate access point or bridge and force them to associate with the attacker's machine. Some tools are:
  - AirJack
  - File2air
  - Libwlan
  - FakeAP
- *Encrypted traffic injection tools:* Once thought impossible, these tools allows you to inject traffic into WEP-protected wireless networks without even knowing the secret key. The only such tool available is called WepWedgie.
- *Access Point Management utilities:* Although access point manufacturers usually provide necessary configuration utilities, or, most likely, the access point will have an easy-to-use configuration interface accessible via a casual Web browser, there are some utilities that can come in handy while auditing access point security. One of such tools is Wireless Access Point Utilities for UNIX.

8. Conclusion

The available number of useful wireless security auditing tools is staggering. Even better, the majority of the most powerful tools are open source and free, which allows you to experiment with them as much as you like and modify the source to suit your specific requirements. If you are a software

developer, you most likely won't need to write your new wireless security tool or library from scratch; there is a fair amount of great code you can use and learn from. Study, categorize, and update your wireless hacking tools and always remember that Black Hats can use the same tools and they do know why, when, and how to use them.

References

Barken, L.,Bermel, E.,Eder, J.,Fanady, M.,Koebrick, A.,Mee, M., Palumbo, M. *"Wireless Hacking :Projects for Wi-Fi Enthusiasts"*. Syngress; 1 edition (October 1, 2004).

Fluhrer, S., Mantin, I., Shamir, A. "Weaknesses in the Key Scheduling Algorithm of RC4", *Eighth Annual Workshop on Selected Areas in Cryptography, 2001*.

Flickenger, R.. *"Wireless Hacks : 100 Industrial-Strength Tips & Tools"*. O'Reilly Media, Inc.; 1 edition (September 16, 2003)

Pahlavan K., Krishnamurthy P. *"Principles of Wireless Networks: A Unified Approach"*. 2001 - Prentice Hall PTR Upper Saddle River, NJ, USA

Sutton, M. "Hacking the Invisible Network". iALERT White Paper, iDefense Labs, 2002. http://www.madchat.org/reseau/wireless/Wireless.pdf

Authorization and Disclaimer