

# Wireless intrusion detection technologies to determine friend or foe

Victor A. Clincy, and Padmaja Mudiraj  
College of Science and Math  
Computer Science and Information Systems Department  
Kennesaw State University  
Kennesaw, Georgia 30144  
[vclincy@kennesaw.edu](mailto:vclincy@kennesaw.edu), 770-420-4440

**Keywords:** *WLAN Security, Intrusion Detection, 802.11 Security*

## 1. Abstract

Wireless Local Area Networks (WLANs) allow devices to connect with a useable amount of bandwidth without being networked via a physical connection. Laptop users within range of the WLAN could connect anywhere and be granted instant access to all networking resources. WLANs, which exist over radio waves, have no physical structure and are therefore more vulnerable to tampering. Therefore, security in the WLANs has come under intense scrutiny.

Though wireless networks have seen widespread acceptance in the home user markets, widely reported and easily exploited vulnerabilities in the wireless security system have decreased wireless' deployment rate in enterprise environments. While many people don't know exactly what the weaknesses are, most have blindly accepted that wireless networks are inherently insecure and nothing can be done to improve the security level. But this is not true. It is recommended to do the basic effort before coming to a conclusion.

This paper addresses the importance of monitoring the wireless networks, and demonstrates how intrusion prevention technology secures the WLANs. Through this paper, we have made an attempt to analyze and asses the performance of some of the wireless intrusion detection tools (Airsnares, AiropEEK NX, and AirPatrol Mobile), describe the pros and cons of these tools, and analyze how the network's security level varies with the deployment of these tools. The paper seeks to assist home/enterprise networks in reducing the risks associated with 802.11 wireless local area networks.

## 2. Methodology

- Analyze how the wireless technology works.
- Investigate wireless security freeware.
- Assess the performance of each of the tools.
- Study the feasibility of these technologies in the near by future.

### **3. Explanation**

#### **3.1. Airopeek NX:**

##### **3.1.1. Basic Features**

Below is a brief description about the functions of Airopeek NX, and some basic features it provides (Geier, 2002).

- The main responsibility of AiroPeek NX is to capture and decode packets. The user configures the parameters which gives the tool the information about the kind of packets to be captured. Depending upon these configured parameters, the Airopeek NX captures the packets and stores them in the memory.
- The flexibility in packet filtering provides the users with the options to set the limitations on the capturing window and to narrow down the search for specific user defined rules. The alarm feature that alerts the occurrence of an unauthorized event (specified by the user) is convenient.
- Termination of the capture can be done either by manually aborting it, or by setting the maximum time frame which indicates the duration of a particular capture. The tool facilitates the storage of the results to a file, which can be retrieved for later analysis.
- Analyzing the results of the captures is much simpler with AiroPeek NX because it highlights the important packets using specific colors that differentiate them from the rest of the routine packets. Moreover, the reports generated provide real-time information about the traffic patterns which include percent of network utilization, number of packets per second, and error per second.
- The capturing of packets (Refer to snapshot-1) is only the first step in analyzing a wireless LAN. The next step is to decode these packets, which is when AiroPeek NX really shines. The tool decodes the protocols and provides the catalog of the packets. The decode view highlights the detailed information of each packet which include source address, destination address, data rate, protocol type, etc (refer to snapshot-2).
- When viewing the details of a packet, AiroPeek NX displays a short summary, including packet length, data rate, signal level, etc.

**Capture 3**

Packets received: 47    Memory usage: 0%  
Packets filtered: 47    Filter state: ← Accept all packets    Start Capture

Packet	Source	Destination	BSSID	Data Rate	Ch
1	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
2	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
3	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
4	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
5	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
6	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
7	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
8	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
9	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
10	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
11	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
12	00:A0:F8:9B:B9:AA	Broadcast	00:A0:F8:8B:20:1F	11.0	

File Adapter: C:\Demo.apc    Packets: 47    Duration: 0:00:01

(Snapshot 1: Summary of the captured packets)

Packet: 35

**Packet Info**

- Flags: 0x00
- Status: 0x00
- Packet Length: 1266
- Timestamp: 16:18:45.410756000 06/06/2001
- Data Rate: 22 11.0 Mbps
- Channel: 11 2462 MHz
- Signal Level: 74%
- Noise Level: 0%

**802.11 MAC Header**

- Version: 0
- Type: %10 Data
- Subtype: %0000 Data Only
- To DS: 0
- From DS: 1
- More Frag.: 0
- Retry: 0
- Power Mgmt: 0
- More Data: 0
- WEP: 0
- Order: 0
- Duration: 218 Microseconds
- Destination: 00:A0:F8:9B:B9:AA
- BSSID: 00:A0:F8:8B:20:1F**
- Source: 00:A0:C5:E2:6D:A8
- Seq. Number: 314
- Frag. Number: 0

(Snapshot 2: Decodes the packet)

### **3.1.2. Pros**

- The tool provides the user with convenient features to monitor and audit the network security
- Users can define the attributes for packet filtering

### **3.1.3. Cons**

- Limited to special radio Network Interface Card (NIC)
- It only runs on Windows 2000 or Windows XP.

## **3.2. Airsnare:**

### **3.2.1. Basic Features**

Below is a brief description about the functions of Airsnare, and some basic features it provides (Wireless Security, n.d.).

- AirSnare is a wireless network monitoring system that has some pretty cool features. The user enters the list of MAC addresses thereby confirming those addresses as the part of their network. Depending on those addresses, the tool monitors the network and alerts the presence of other MAC addresses which are not the part of the specified list (refer to snapshot-3). The software also provides additional facilities such as audio alerting and emailing the information about the security breaches.
- Another special feature is the “Airhorn”, an element of AirSnare that allows the user to send intruders a message that pops-up on their screen telling them what ever you type in, for example "Your illegal activities have been detected, so get off of my network".
- Before you download the AirSnare, you have to download, and install the WinPcap library. It's a protocol analyzer and is an important component in AirSnare. It doesn't install a program just a library that AirSnare uses to capture network packets.

Detected possible unfriendly MAC addresses: 3

Network Adapters		Date	Src MAC	Src IP	Event	Dst MAC
(1) Generic NdisWan adapter		9/16/2005 1:50:55 PM	00600FB53D...	57.80.136.9	=SSL(SHTM...	00022D6EE
(2) ORINOCO PC Card (Microsoft's Packet Scheduler)		9/16/2005 1:50:54 PM	00600FB53D...	57.80.136.9	=SSL(SHTM...	00022D6EE
(3) NET IP/1394 Miniport		9/16/2005 1:50:54 PM	00600FB53D...	57.80.136.9	=SSL(SHTM...	00022D6EE
(4) 3Com EtherLink PCI (Microsoft's Packet Scheduler)		9/16/2005 1:50:54 PM	00600FB53D...	57.80.136.9	=SSL(SHTM...	00022D6EE
Unfriendly MAC Addresses		9/16/2005 1:50:54 PM	00600FB53D...	57.80.136.9	=SSL(SHTM...	00022D6EE
00022D6E8A5A - sadhu.launchmodem.com		9/16/2005 1:50:45 PM	00600FB53D...	207.46.2.48	MSN Msg	00022D6EE
00904B003B74 - 192.168.2.1		9/16/2005 1:50:42 PM	00600FB53D...	216.155.193.171	=>	00022D6EE
00600FB53DE0 - 57.80.136.9		9/16/2005 1:50:02 PM	00600FB53D...	207.46.2.48	MSN Msg	00022D6EE
Friendly MAC Addresses		9/16/2005 1:50:02 PM	00600FB53D...	192.168.1.254	=DNS=>	00022D6EE
00-02-2D-6E-8A-5A		9/16/2005 1:50:02 PM	00600FB53D...	192.168.1.254	=DNS=>	00022D6EE
		9/16/2005 1:50:02 PM	00600FB53D...	216.155.193.171	=>	00022D6EE
		9/16/2005 1:50:02 PM	00600FB53D...	206.190.50.162	=SSL(SHTM...	00022D6EE
		9/16/2005 1:50:02 PM	00600FB53D...	207.46.2.48	MSN Msg	00022D6EE

Scanning Network Traffic on (2) ORINOCO PC Card (Microsoft's Packet Scheduler) | Watching: 00600FB53DE0 | Packets: 100

(Snapshot 3: Displays the detected unfriendly MAC addresses)

### 3.2.2. Pros

- It's free, and works with most wireless cards. It will tell you who is connected to your wireless network; all based on MAC addresses and IP numbers. It keeps continuous log in logs folder.
- It is easy to use and if you have a wireless network, you think it could be an invaluable tool for maintaining tight security

### 3.2.3. Cons

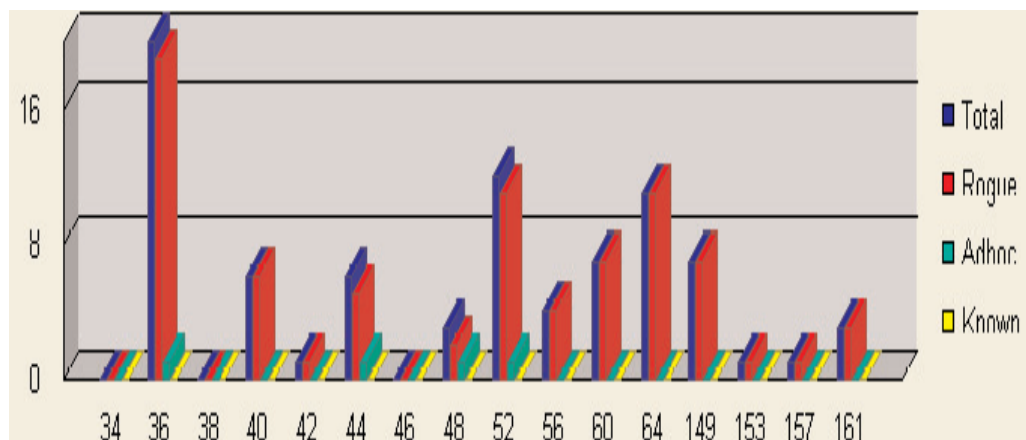
- As we mentioned before, Airsnare has a special feature that allows to send a message to an unfriendly MAC/IP. But, to use this functionality, AirSnare must be running on a Windows NT, Windows 2000 or a Windows XP machine. In order for the intruder to see this message, they also must be running NT, 2000 or XP.

## 3.3. AirPatrol Mobile:

### 3.3.1. Basic Features

Below is a brief description about the functions of AirPatrol Mobile, and some basic features it provides (AirPatrol Mobile, n.d.).

- The AirPatrol Mobile detects and locates rogue access points. It enables you to detect and locate wireless laptops, rogue access points and all other wireless devices, and see exactly where they are.
- It provides you with complete site-survey data, showing all access points and laptops. All available data for all discovered devices is displayed including SSID, signal strength, MAC Address, and connected access point SSID.
- It provides detailed wireless signal strength maps, which help you determine areas of poor coverage, and enable you in placing the wireless network assets efficiently (refer to snap shot 4).



(Snapshot 4: Displays the total known, rouge devices, etc. Reference: <http://www.operativesoft.com/Product/apmobile.pdf>)

### 3.3.2. Pros

- It accurately detects, locates, and visually displays all wireless devices
- It is quick and easy to set up
- It graphically displays channel utilization
- It conduct site surveys for wireless network planning and monitoring
- It includes powerful reporting and logging tools to help you comply with Sarbanes Oxley or HIPAA requirements.

### 3.3.3. Cons

- Although the program is easy to use and relatively effective at pinpointing the location of access points and ad hoc networks, administrators looking for in-depth radio-frequency analysis tools or constant detection capabilities should look elsewhere.

- It cannot perform the kind of in-depth RF analysis, and it cannot detect interference issues.

#### **4. Future feasibility of the technologies**

From a security viewpoint, organizations need to be able to monitor and manage the radio frequency footprint of their buildings. Continuous monitoring enables the network administrator to identify not only authorized wireless access points and clients but also rogue devices being used to gain access to the network. This means that even in its very basic mode of operation, the network monitoring tools can help to identify trusted devices and determine friend from foe.

Therefore, wireless intrusion detection systems (IDS) are an important addition to the security of wireless local area networks. Of course, just as with a wired network, an IDS is only one part of a greater security solution. WLANs require a number of other security measures to be employed before an adequate level of security can be reached, but the addition of a wireless IDS can greatly improve the security posture of the entire network.

If you have a wireless network, the tools described in this paper are powerful network planning and tuning tools to help you diagnose and correct wireless network problems. They are invaluable for planning future wireless network deployments and for conducting site surveys.

#### **5. References**

- 1) AiroPeek NX. (n.d). *WildPackets*.  
<http://www.wildpackets.com/products/demos/apwnx>
- 2) AirSnare-Intrusion detection software for windows. (n.d).  
<http://home.comcast.net/~jay.deboer/airsnare/download.html>
- 3) AirPatrol. (n.d). *Operative Software Products*.  
<http://www.operativesoft.com/html/airpatrol.htm>
- 4) Geier, Jim. (2002, June). AiroPeek NX. *Wi-Fi Planet*.  
<http://www.wi-fiplanet.com/reviews/article.php/1268971>
- 5) Wireless Security. (n.d). *WorldStart.Com*. <http://www.worldstart.com/tips/tips.php/172>
- 6) AirPatrol Mobile. (n.d). *Cirond Corporation*.  
<http://www.operativesoft.com/Product/apmobile.pdf>
- 7) AirPatrol Mobile Images Wireless Nets. (n.d). *eWeek.Com*.  
<http://www.eweek.com/article2/0,1895,1610085,00.asp>