Applied Methodologies, Inc.

Wireless Security Audit produced for New York Incurance Co.

January 2003

Table Of Contents

Introduction

Applied Methodologies, Inc. (AMI) has identified several potential security weaknesses in NY Insurance (NYI) Wireless LAN infrastructure. AMI has discovered these weaknesses during a routine audit of one of its other client's wireless networks. The information included in this report is to be deemed informational and can be used as an initial step to further securing NYI's wireless network.

Disclaimer

AMI has no intent or never attempted to scan and obtain the information outlined in this report purposely without the consent of the owners of the equipment listed in such report. The information gathered in this report was obtained during a routine security audit and was included automatically without AMI's knowledge from the result of the technology's radio broadcast nature. AMI is providing this information to the owners of such equipment in the spirit of security information awareness.

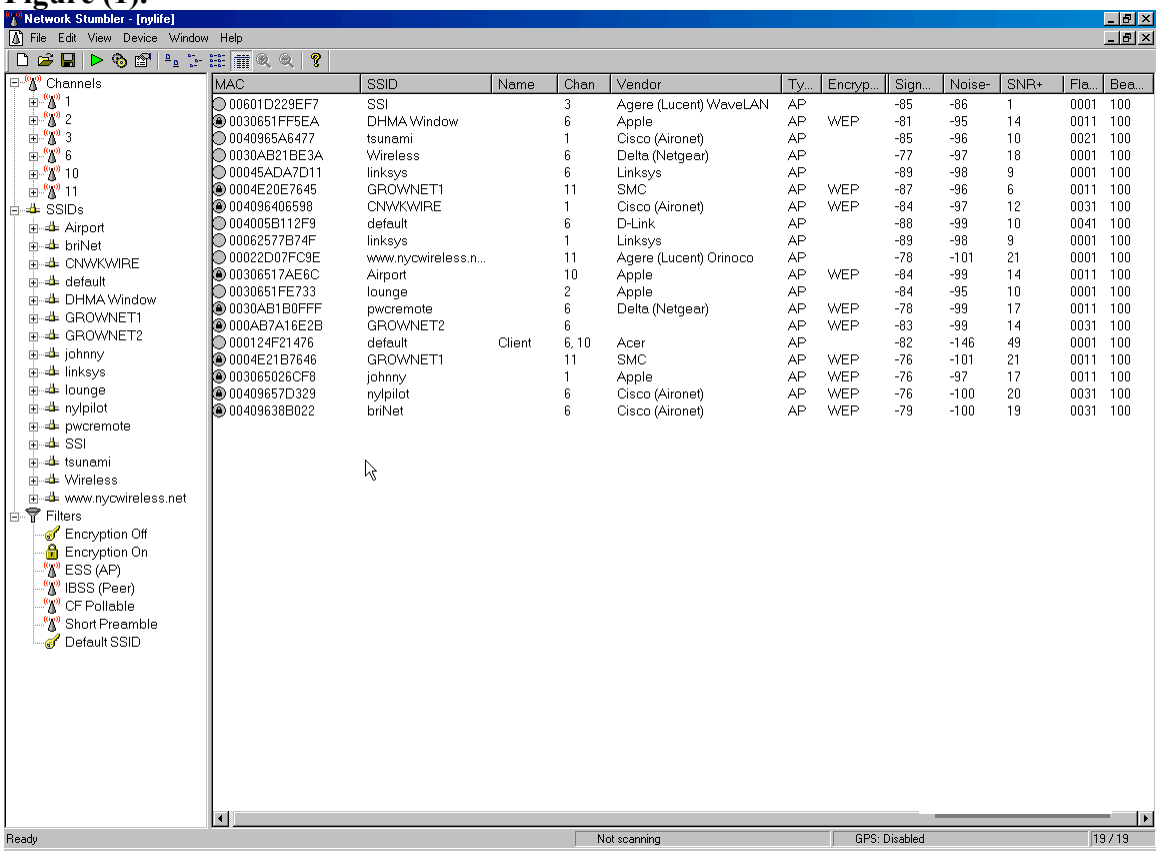
AMI never used any of the tools mentioned in this report to crack passwords or deny service to the equipment mentioned in this report. AMI will only demonstrate such security issues outlined in this report only with the consent of the owners of the equipment outlined in this report.

Wireless Enumeration tool

AMI uses a popular shareware tool called NETSTUMBLER to perform a basic Access Point(AP) inventory and identify rogue Access Points. It was during this activity the NYI APs were identified based on the proximity of the scanning.

The following screenshot outline the NYI APs identified using Netstumbler.

Figure (1).



What this displays shows is all of the Cisco Aironet APs that have WEP enabled. The second column SSID shows the SSID Ids of nypilot. The other AP names may belong to NYI. This information was picked up on the next block, across the street and up to a block away from NYI's 51 main office building.

What does this mean?

NYI's wireless LAN infrastructure is emitting its radio waves out into the street and down the block. This is normal behavior due to the amount of Access Points(AP) and the amount of wattage/dBs emitted. However, due to diffraction and refraction from the buildings in the local neighborhood NYI's signals are focused down blocks where they can be picked up easily. This makes it very easy for anybody with a homebrew Omni Directional, Directional or Yagi antenna to perform forensic protocol analysis to crack the WEP keys and easily gain access to the NYI infrastructure. This type of activity can be demonstrated by AMI. The use of WEP keys does not guarantee any high level of security at all. Due to the amount of APs and channels used, someone in one of the park across the street or someone down the block can obtain enough information about NYI's network to launch an attack against NYI resources, use NYI's network for free internet access, or launch attacks from NYI's network via the wireless network. NYI's building may be acting like one large transmitter around its city campus.

How is this possible?

First look at the Beacon column in Figure(1). (The column labeled Bea at the far right) This indicates that your APs are possibly in a passive scanning mode. Beacons (short for Beacon Management frame) are short frames that are sent from the access point to the stations in Infrastructure mode or Ad Hoc mode in order to organize and synchronize wireless communication on the LAN. Beacons serve several functions, including the following.

- Time synchronization for FHSS based systems.
- FH or DS for dwell and hop times or in a DS based system channel information
- SSID information
- TIM (traffic indication map)
- Supply supporting rates for rate adjustment for longer distance clients and roaming.

The passive scanning mode configuration is not the real issue but what is contained in the beacons(sent every 100ms from clients and AP) or other management frames(probes, association requests etc) that crackers use to gain access to your network. Setting the access points to Active Scanning mode, where clients initiate the process would help conceal the wireless network. Active scanning involves the sending of a probe request frame from a wireless station. Actually that is what the AP enumeration tools do, listen for beacons and send probe frames. Stations send this probe frame when they are actively seeking a network to join. The probe frame will contain the SSID of the network they wish to join or a broadcast SSID. If a probe request is sent specifying an SSID, then only access points that are servicing that SSID will respond with a probe response frame. If a probe request frame is sent with a broadcast SSID, than all access points within reach will respond with a probe response frame. The signal strength of the probe response frames that the PC card receives backs helps determine the AP with which the wireless client will attempt to associate. The client generally chooses the AP with the strongest signal strength and lower BER. The BER is a ratio of corrupted packets typically determined by the Signal-to-Noise-Ratio of the signal. If the peak signal level of an RF signal is somewhere near the noise floor, the receiver may confuse the data signal with noise.

Because the NYI wireless network is using several channels overlapping and non-overlapping, the amount of intentional radiator traffic seeping onto the street in beacons and possibly data traffic is easily picked up.

In Figure(1). shown earlier if you notice the columns titled Signal+ Noise- SNR+ you will see the various signal strengths measured in dBm. The significant column is the SNR+ the higher that number the better the delta in dBm from the noise floor(column Noise-) and an actual decent signal from the AP(Signal+ column). The lower the (-) signal number towards 0 then up in dBm means a better signal and the higher the noise number in (-) heading away from 0 and positive dBm means that this signal has less noise and is of better quality. The SNR(Signal to Noise Ratio) is the delta number in between.

You will notice some APs in the 20s and there is one in the forties listed below which are the best APs with the highest SNR+, meaning that these are the best APs to focus an antenna on for its signal level is decent enough to use a sniffer and other tools to gain access. With the right antenna and receive sensitivity settings on a PC card better signals can be achieved from a distance. Table 1.0 below lists the best NYI APs found picked up accidentally during AMI's wireless scan.

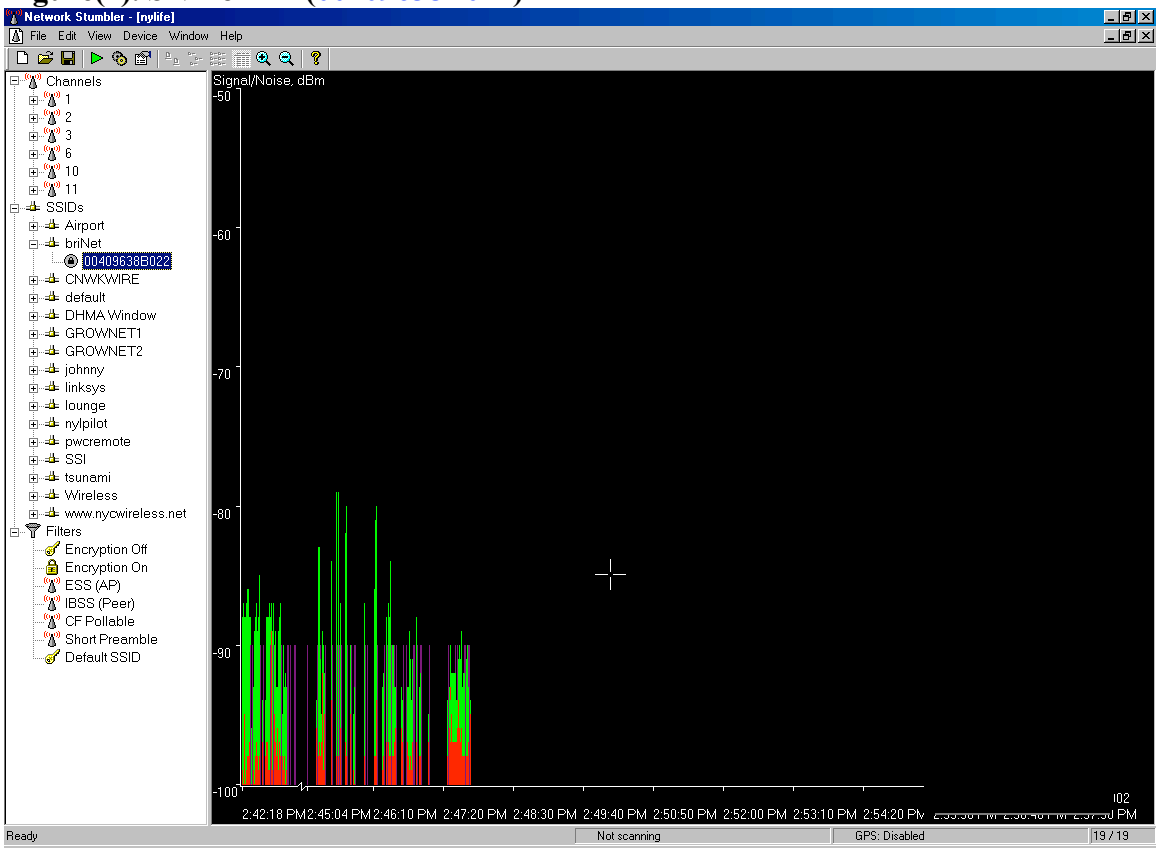
Table 1.0

AP MAC address	Channel	Signal+	Noise-	SNR+
00409657D329	**6**	**-76**	**-101**	**21**
000124F21476	**6,10**	**-82**	**-146**	**49**
00409638B022	**6**	**-79**	**-100**	**19**
0040965A6477	**1**	**-85**	**-96**	**10**

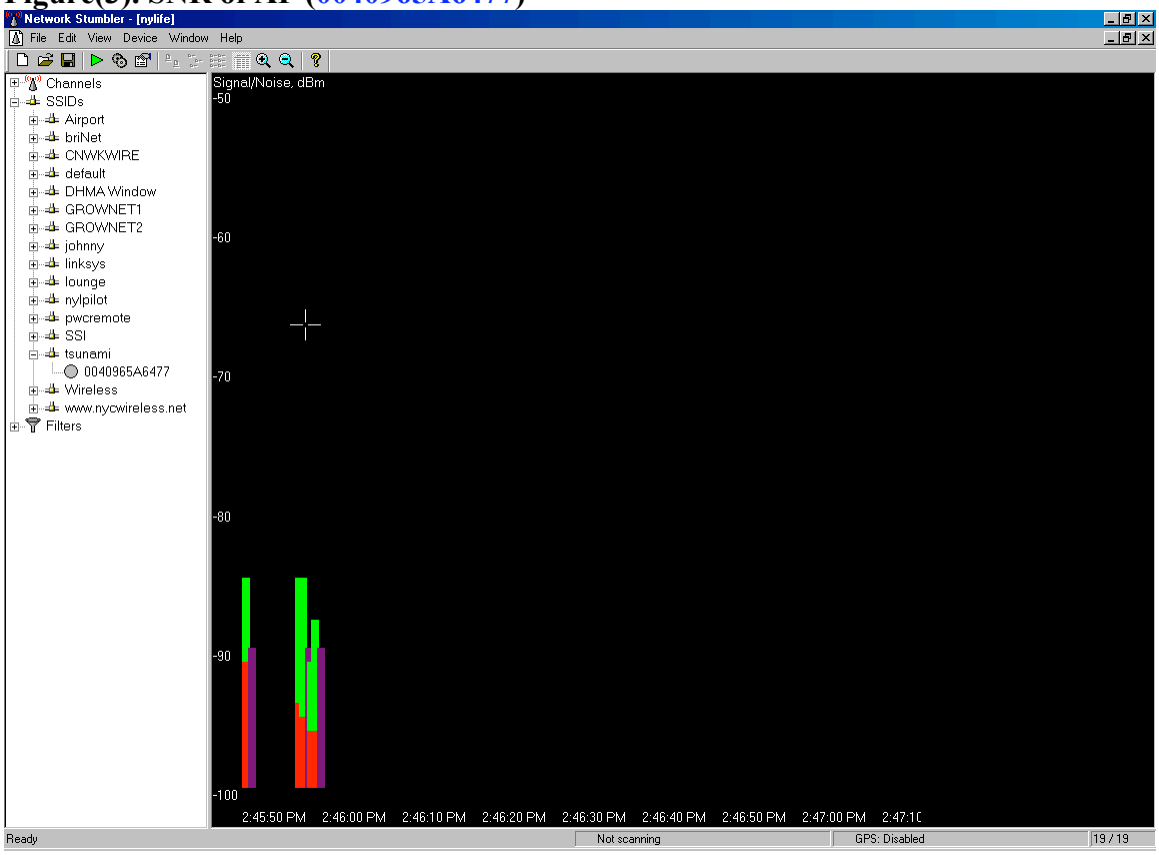
Figure(2) and (3) below shows the SNR in graphical form of the AP with the MAC address of **00409638B022** and a SNR of **19** compared to another AP with the MAC address of **0040965A6477** with a SNR of **10**.

Notice that the AP with the SSID of **tsunami**, this is the default SSID for a Cisco AP. This could be a rogue AP within NYI with no WEP security measures enabled thus creating a back door into NYI. The other APs listed in Figure(1). Could also be in NYI and should be checked into.

Figure(2). SNR of AP (00409638B022)



Figure(3). SNR of AP (0040965A6477)



Even though the signals are weak, with off the shelf equipment, PC cards, antennas etc a hacker can tune the equipment to hear theses weak signals. A commercial antenna, directional(or home made out of an Pringles potato chip can) or Yagi can be used to focus the beamwidth from the AP and or focus the EIRP antenna used by the hacker sending the probe packets sent from the hackers wireless laptop to provide enough dBm gain from a distance to try to break NYI's wireless security from a safe and distant location.
See the recommendations section later in this report about cell sizing to help redress this issue.

Access Point Association and Authentication exploits

There are two types of AP authentication during the association process, Open system Authentication Process and Shared Key Authentication Process

The Open System Authentication Process occurs as follows:

1. The wireless client makes a request to associate to the access point
2. The access point authenticates the client and sends a positive response and the client becomes associated(connected)

Open System authentication is a very simple process. Wireless LAN products have the option of using WEP encryption with Open System authentication. If WEP is used with the Open System authentication process, there is still no verification of the WEP key on each side of the connection during authentication. Rather, the WEP key is used only for encrypting data once the client is authenticated and associated.

Open System authentication is used in several scenarios, but there are two main reasons to use it. First, Open System Authentication is considered the more secure of the two available authentication methods for reasons explained below. Second, Open System authentication is simple to configure because it requires no configuration at all. All 802.11 compliant wireless LAN hardware are configured to use Open System by default, thus making it easy to get started with building your wireless network.

Shared Key Authentication

Shared key authentication is a method of authentication that requires the use of WEP. WEP encryption uses keys that are entered manually into both the client and the AP. These keys must match on both sides for WEP to work properly. Shared key authentication uses WEP keys in two fashions, as is described next.

Shared Key Authentication process:

The authentication process using Shared Key authentication occurs as follows:

1. A client requests association to an access point - this step is the same as that of Open System authentication.
2. The access point issues a challenge to the client – this challenge is randomly generated in plain text, which is sent form the access point to the client in the clear.
3. The client responds to he challenge - the client responds by encrypting the challenge text using the client's WEP key and sending it back to the AP.
4. The AP responds to the client's response - the AP decrypts the client's encrypted response to verify that the challenge text is encrypted using a matching WEP key.

Through this process the AP determines whether or not the client has the correct WEP keys. If the client's WEP keys is correct, the AP will respond positively and authenticate the client. If the client's WEP key is incorrect, the AP will respond negatively, and not authenticate the client, leaving the client unauthenticated and unassociated.

It would appear that the Shared Key authentication process is more secure than that of Open System authentication, but it is not. Rather, Shared Key authentication opens the door for hackers. It is important to understand both ways WEP is used. The WEP key can be used during the Shared Key authentication process to verify a client's identity, but it can also be used for encryption of the data payload sent by the client though the AP. Shared Key authentication is not considered secure because the AP transmits the challenge text in the clear and receives the same challenge text encrypted with the WEP key. This defeats the cipher stream for it is reversible. This scenario allows a hacker using a sniffer on the street below NYI to see both the plaintext challenge and the encrypted challenge. Having both of these values, a hacker could use a simple cracking program like WEPCRACK to derive the WEP key. Once the WEP key is obtained, the hacker could decrypt encrypted traffic. It is for this reason that open system authentication is considered more secure than Shared Key Authentication.

As discussed earlier in this document and shown in Figure(1) the SNR of the AP could be obtained so the hacker could determine the AP with the best signal strength to remotely work from. The nature of DSSS carrier frequencies and 802.11's rate adjustment features via the beacon and probing process enable a wireless client to access a network at distances over a mile away but at the reduced speed of 1Mbs. If NYI is using the rate adjustment feature based on the signal strength and BER then NYI should consider turning off certain rates in their APs to prevent this from happening, thus rendering such potential attacks out of range.

As of this writing AMI is unaware of what method NYI is using for wireless client authentication. In light of the contrasting operation of these methods NYI should consider reviewing their wireless client authentication process to ensure that the more secure method is utilized.

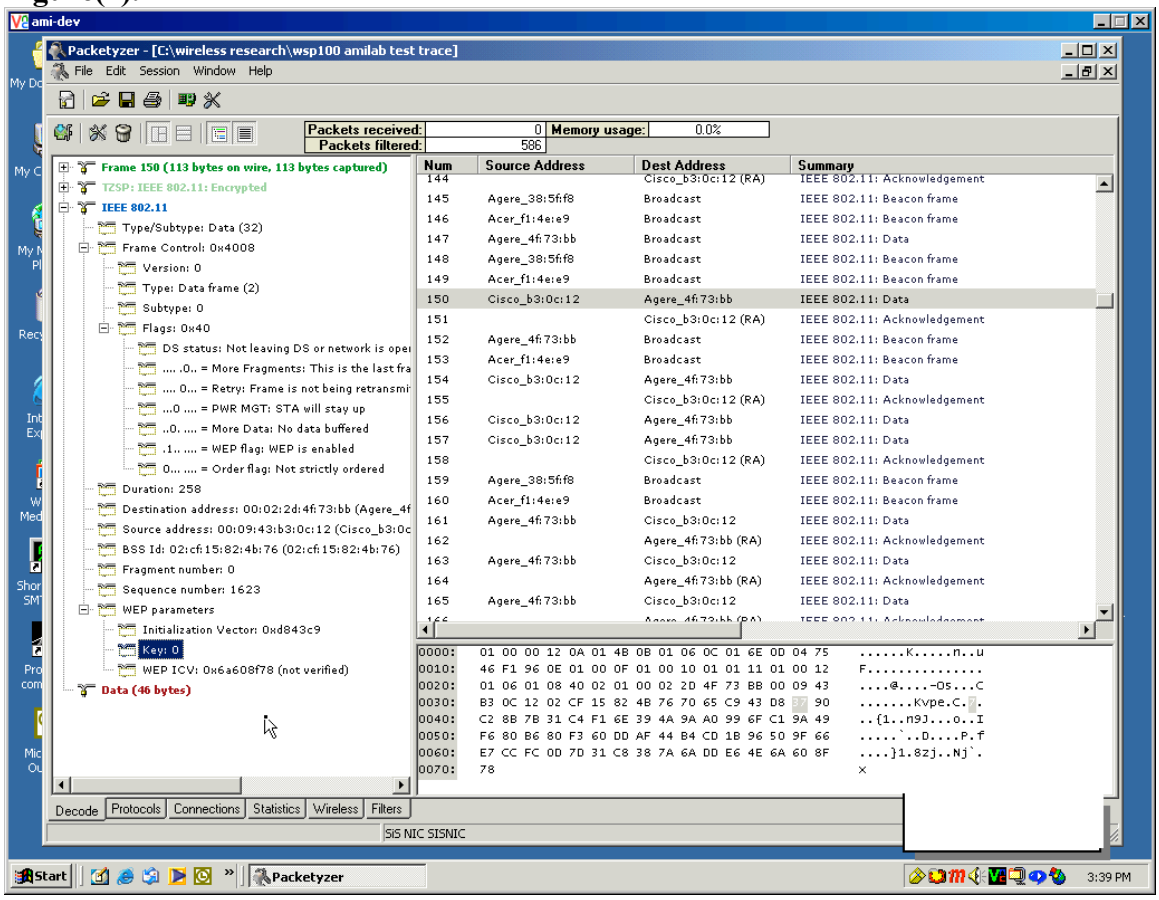
WEP Exploits

The WEP keys can be easily cracked due to the amount of leaked radio traffic onto the street.

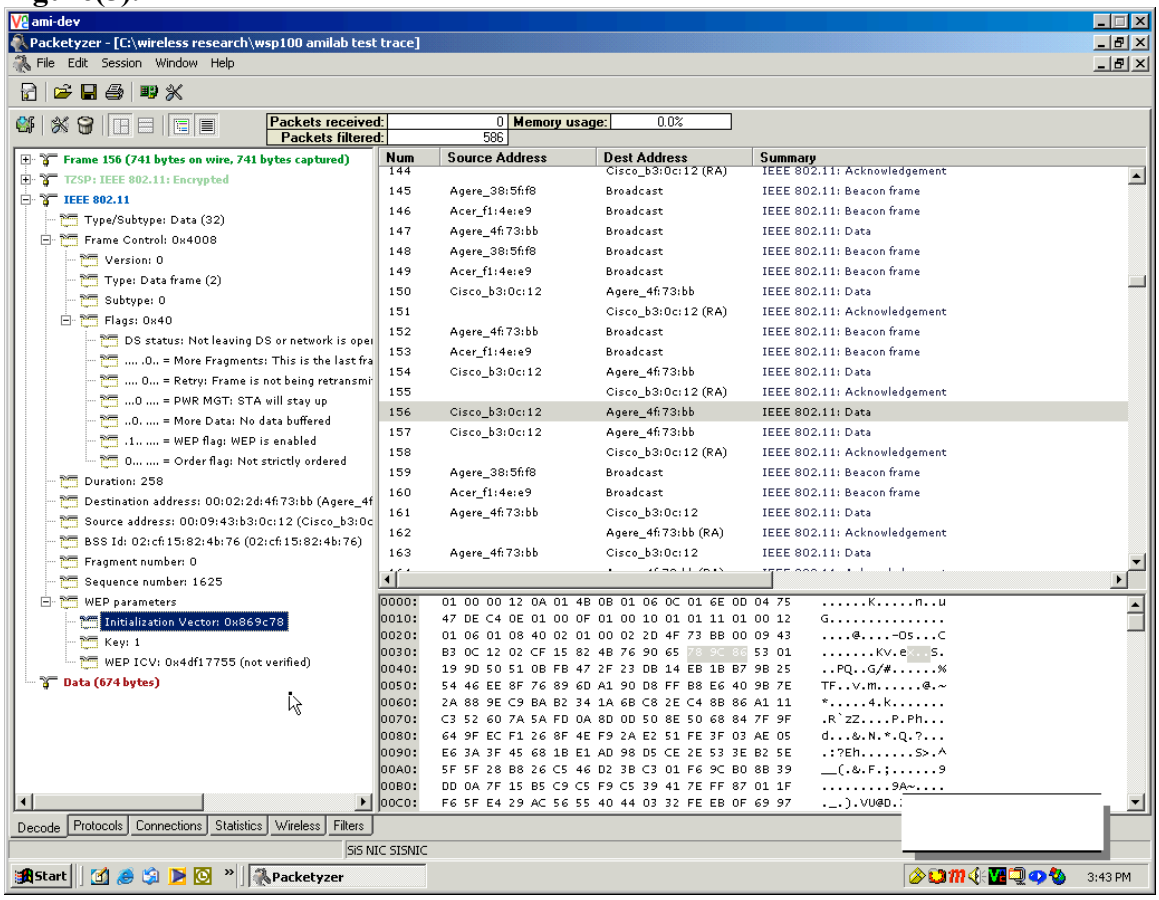
Wired Equivalent Privacy (WEP) is an encryption algorithm used by the Shared Key authentication process of authentication users and for encrypting data payload over only the wireless segment of the LAN. The IEEE 802.11 standard specifies the use of WEP. WEP is a simple algorithm that utilizes a pseudo-random number generator (PRNG) and the RC4 stream cipher. For several years this algorithm was considered a trade secret and details were not available, but in September of 1994, someone posted the source code in the CYPHERPUNKS mailing list. Although the source code is now available, RC4 is still trademarked by RSADSI. The RC4 system cipher is fast to decrypt and encrypt, which saves on CPU cycles, and RC4 is also simple enough for most software developers to code it into software.

When WEP is referred to as being simple, that means that it is weak. The RC4 algorithm was inappropriately implemented in WEP, yielding a less than adequate security solution for 802.11 based networks. Both 64 bit and 128 bit WEP have the same weak implementation of a 24 Initialization Vector (IV) and use the same flawed process of encryption. The flawed process is that most implementations of WEP initialize hardware using an IV of 0 - thereafter incrementing the IV by 1 for each packet sent. See Figure(4) and Figure(5) which depict a packet trace using a low cost wireless sniffer viewing the IV sequence.

Figure(4).


ami-dev
Packetyzer - [C:\wireless research\wsp100 amilab test trace]
File Edit Session Window Help
Packets received: 0
Packets filtered: 586
Memory usage: 0.0%
Frame 150 (113 bytes on wire, 113 bytes captured)
TZSP: IEEE 802.11: Encrypted
IEEE 802.11
Type/Subtype: Data (32)
Frame Control: 0x4008
Version: 0
Type: Data frame (2)
Subtype: 0
Flags: 0x40
DS status: Not leaving DS or network is oper
.... .0.. = More Fragments: This is the last fra
.... 0... = Retry: Frame is not being retransmi
...0 .... = PWR MGT: STA will stay up
..0. .... = More Data: No data buffered
.1.. .... = WEP flag: WEP is enabled
0... .... = Order flag: Not strictly ordered
Duration: 258
Destination address: 00:02:2d:4f:73:bb (Agere_4f
Source address: 00:09:43:b3:0c:12 (Cisco_b3:0c
BSS Id: 02:cf:15:82:4b:76 (02:cf:15:82:4b:76)
Fragment number: 0
Sequence number: 1623
WEP parameters
Initialization Vector: 0xd843c9
Key: 0
WEP ICV: 0x6a608f78 (not verified)
Data (46 bytes)
Num Source Address Dest Address Summary
144 Cisco_b3:0c:12 (RA) IEEE 802.11: Acknowledgement
145 Agere_38:5f:f8 Broadcast IEEE 802.11: Beacon frame
146 Acer_f1:4e:e9 Broadcast IEEE 802.11: Beacon frame
147 Agere_4f:73:bb Broadcast IEEE 802.11: Data
148 Agere_38:5f:f8 Broadcast IEEE 802.11: Beacon frame
149 Acer_f1:4e:e9 Broadcast IEEE 802.11: Beacon frame
150 Cisco_b3:0c:12 Agere_4f:73:bb IEEE 802.11: Data
151 Cisco_b3:0c:12 (RA) IEEE 802.11: Acknowledgement
152 Agere_4f:73:bb Broadcast IEEE 802.11: Beacon frame
153 Acer_f1:4e:e9 Broadcast IEEE 802.11: Beacon frame
154 Cisco_b3:0c:12 Agere_4f:73:bb IEEE 802.11: Data
155 Cisco_b3:0c:12 (RA) IEEE 802.11: Acknowledgement
156 Cisco_b3:0c:12 Agere_4f:73:bb IEEE 802.11: Data
157 Cisco_b3:0c:12 Agere_4f:73:bb IEEE 802.11: Data
158 Cisco_b3:0c:12 (RA) IEEE 802.11: Acknowledgement
159 Agere_38:5f:f8 Broadcast IEEE 802.11: Beacon frame
160 Acer_f1:4e:e9 Broadcast IEEE 802.11: Beacon frame
161 Agere_4f:73:bb Cisco_b3:0c:12 IEEE 802.11: Data
162 Agere_4f:73:bb (RA) IEEE 802.11: Acknowledgement
163 Agere_4f:73:bb Cisco_b3:0c:12 IEEE 802.11: Data
164 Agere_4f:73:bb (RA) IEEE 802.11: Acknowledgement
165 Agere_4f:73:bb Cisco_b3:0c:12 IEEE 802.11: Data
0000: 01 00 00 12 0A 01 4B 0B 01 06 0C 01 6E 0D 04 75 ......K.....n..u
0010: 46 F1 96 0E 01 00 0F 01 00 10 01 01 11 01 00 12 F...............
0020: 01 06 01 08 40 02 01 00 02 2D 4F 73 BB 00 09 43 ....@....-Os...C
0030: B3 0C 12 02 CF 15 82 4B 76 70 65 C9 43 D8 90 ....Kvpe.C..
0040: C2 8B 7B 31 C4 F1 6E 39 4A 9A A0 99 6F C1 9A 49 ..{1..n9J...o..I
0050: F6 80 B6 80 F3 60 DD AF 44 B4 CD 1B 96 50 9F 66 .....`..D....P.f
0060: E7 CC FC 0D 7D 31 C8 38 7A 6A DD E6 4E 6A 60 8F ....}1.8zj..Nj`.
0070: 78 x
Decode Protocols Connections Statistics Wireless Filters
SiS NIC SISNIC
Start Packetyzer 3:39 PM

Figure(5).



For a busy network, statistical analysis shows that all possible IVs of (2 to the 24th) would be exhausted in 5 hours, meaning the IV would be reinitialized starting at zero at least once every 5 hours. This scenario creates an open door for hackers. When WEP is used, the IV is transmitted in the clear with each encrypted packet. The manner in which the IV is incremented and sent in the clear allows the following breaches in security:

- Active attacks to inject new traffic - Unauthorized mobile stations can inject packets on the network based on know plaintext.

- Active attacks to decrypt traffic – Based on tricking the access point.

- Dictionary building attacks - After gathering enough traffic, the WEP key can be cracked using freeware tools like WEPCRACK. Once the WEP key is cracked, real time decryption of packets can be accomplished by listening to packets using the WEP key.

- Passive attacks to decrypt traffic – Using statistical analysis, WEP traffic can be decrypted. Performing a search on the Internet in regards to cracking WEP will yield many articles and simple downloadable tools to accomplish this.

An example relative to NYI

With a laptop a hacker can sit outside(across the street, in the park, down the block or even in one of the restaurants across from NYI) of NYI's main office location, trace packets using tools like Packetyzer, Linkferret, AirSnort, Kismet, and dump the resulting packet traces into a WEP cracking tool such as WEPCRACK which runs on the LINUX platform. In several hours the hacker can have the WEP keys needed to add to his wireless card. The hacker can then use a regular shareware sniffer such as Etherreal, Analyzer or Packetyzer and can now see all traffic traversing NYI's wireless network unencrypted. If NYI's Access Points provide IP addresses via DHCP or a DHCP server is available on the wireless segment the hacker can obtain a NYI IP address and become just like any other internal client on the NYI network.

This is just as if NYI left an RJ-45 cable on the street that is connected to one of its backbone switches. The Hacker can now use NYI's network for free internet access, launch attacks via NYI's network or try to gain access to NYI's servers by sniffing for passwords. The hacker can gain access to all routers, switches, Unix servers and any other device that uses Telnet, which transmits keystrokes in clear text. The hacker can now see the Network Neighborhood of NYI servers by discovering Network Name broadcasts etc. NYI's CID organization may use laptops with wireless cards to roam the building and access critical devices during the day for enhanced support.

Another example is that a hacker across the street(maybe from the park) can just filter for Telnet once he/she has the WEP keys. Using a tool that cracks Cisco router and switch passwords called Getpass from Boson, all the hacker has to do is filter for telnet from any Cisco address and capture a SH RUN. The password in the SH RUN is still encrypted yet if the ciphertext of the Enable password in the SH RUN output is imputed into Getpass, Getpas will reveal the Enable password. Figure(6) below displays a sample screenshot of Getpass in action.

Figure(6).

As of this writing it is unsure if NYI has any additional security on its wireless LAN other than WEP keys. It is also unsure if the WEP keys are changed periodically to thus reduce the chances of this attack to happen. AMI can demonstrate these types of issues for NYI at its convenience.

Other types of attacks

Jamming

This entails disrupting the radio signal to cause errors or make the wireless network useless. Considering the equipment needed and the reasonable gain from such an attack is minimal this kind of attack is usually very rare.

Man-in-the-middle Attacks

A man in the middle attack is a situation in which a malicious individual uses an access point to effectively hijack mobile nodes by sending a stronger signal than the legitimate access point is sending to these nodes. The mobile nodes then associate to this rogue access point, sending their data, possibly sensitive data, into the wrong hands. The person perpetrating this type of attack would have to know the SSID, which is easily obtained. Many times a man in the middle attack can be orchestrated using a single laptop computer with two pcmcia cards. Access point software is run on the laptop computer where one pcmcia card is used as an AP and the second card is used to connect the laptop to nearby legitimate access points. This configurations makes the laptop a man in the middle operating between clients and legitimate AP.

A sniffer can also run on this laptop. One particular problem with the man in the middle attack is that the attack is undetectable by users. This type of attack is also unlikely due to the need to generate a more powerful signal. This is very difficult to do with a mobile unit outside a building unless the unit is in a automobile running off the automobile's power.

MAC address spoofing

This type of attack involves listening for know used MAC addresses in the wireless cell and assigning the use of a MAC address to the hacker’s laptop for access during off hours into the corporate wireless network. The reason MAC spoofing is used is to circumvent any known MAC filtering on the AP or MAC logging. This way to any security systems in place the activity of the hacker will look like any legitimate wireless user. This type of attack is used often once the hacker has access to the wireless network.

Many of the common types of attacks and cracks found to be used on a wired network over the internet are fully applicable on a wireless network even more so since the wireless network is usually behind the corporate DMZ thus defeating any of the IDS, Firewall and proxy systems put into place.

Recommendations

There are many methods to mitigate the scenarios listed earlier and to isolate and secure your wireless network considering how easy it is to break into a wireless network. The inherent nature of radio communications makes total secure operation difficult so there is no single one solution to safeguard a wireless network. However, by combining the recommendations outlined below in a manner that is suited to NYI's network security policy significant additional protection can be added to NYI's wireless network. AMI can be available at NYI's convenience to assist in identifying these weaknesses and correcting them.

Rotating WEP static keys

By changing WEP keys periodically NYI can reduce the chances of such keys being cracked using tools off the Internet. Doing this on a small number of APs and clients can be done in a short time manually with a simple process to update users wireless card software.

For a larger number of APs and wireless users in NYI's case the use of a Key Distribution System to provide and rotate WEP keys periodically thus to reduce the chance of active WEP cracking. A Radius or Cisco Secure ACS/AAA server could used for this purpose so authentication to the AP and also for the AP to receive new keys periodically can be done automatically.

Centralized Encryption Key Servers

For enterprise wireless LANs using WEP as a basic security mechanism, centralized encryption key servers should be used if possible for the following reasons:

- Centralized key generation
- Centralized key distribution
- Ongoing key rotation
- Reduced key management overhead

Any number of different devices can act as a centralized key server. Usually a server of some kind of such as a Radius server or a specialized application server for the purpose of handing out new WEP keys on a short time interval is used. Normally when using WEP the keys (made up by the administrator) are manually entered into the stations and APs. When using a centralized key sever an automated process between stations APs and the key server performs the task of handing out WEP keys. Centralized key servers allow for key generation on a per packet(increased overhead)or per session (less overhead) or other methods depending on the particular manufacture's implementation Per –packet WEP key distribution calls for a new WEP key to be assigned to both ends of the connection for every packet sent, whereas per-session WEP key distribution uses a new WEP key for each new session between nodes. Of course internal security around your

centralized key server is critical for if the central key server has failed or become compromised in any way could disrupt the function of your wireless network. Depending on the importance of your wireless network dual/redundant key distribution servers should be considered.

Advanced Encryption Standard or WEPv2 and 802.11i

The Advanced Encryption Standard (AES) is gaining acceptance as an appropriate replacement for the RC4 algorithm used in WEP. AES uses the Rijndale(pronounced RINE-dale)algorithm in he following specified key lengths:

- 128-bit
- 192-bit
- 256-bit

AES is considered to be un-crack able by most cryptographers and the national Institute of Standards and Technology(NIST) has chosen AES for the Federal Information Processing Standard, or /FIPS. As part of the effort to improve the 8o2.11 standard, the 802.11i working committee is considering the use of AES in WEPv2.

AES if approved by the 802.11i working group to be used in WEPv2, will be implemented in firmware and software by vendors. Access point firmware and client station firmware(the pcmcia radio cards) will have to be upgraded to support AES. Client stations software (drivers and client utilities)will support configuring AES with secret keys(s).

Temporal Key integrity Protocol (TKIP)

TKIP is essentially an upgrade to WEP that fixes know security problems in WEP's implementation of the RC4 stream cipher. TKIP provides for initialization vector hashing to help defeat passive packet snooping. It also provides a Message Integrity Check to help determine whether an unauthorized user has modified packets by injecting traffic that enables key cracking. TKIP includes use of dynamic keys to defeat capture of passive keys, a widely publicized hole in the existing WEP standard.

TKIP can be implemented through firmware upgrades to access points and bridges as well as software and firmware upgrades to wireless client devices. TKIP specifies rules for the user of initialization vectors, re-keying procedures based on 802.1x, per packet key mixing, and message integrity code(MIC). There will be a performance loss when using TKOP, due to the overhead on the packets , but this performance decrease may be a valid trade-off, considering the gain in network security.

NYI should check with their wireless manufacture's for details on progress with their products and these emerging security standards.

Filtering techniques

Filtering is a basic security measure that can be combined with others methods listed in this report to further lock down your wireless network. Some filtering methods are listed below:

SSID filtering is a rudimentary method of filtering and should only be used for the most basic access control The SSID is just another term for the network name. The SSID on the AP must match that on the wireless laptop in order for the client to authenticate and associate to the AP. Since SSIDs are broadcast in every beacon frame every 100ns it is simple to find the SSID with any shareware wireless sniffer and even the tools that come standard with many wireless cards.

If your access pints have the ability to remove SSIDs from beacons ad probe responses configure them that way. This configuration aids in deterring the casual or intentional eavesdroppers from trying to gain access to the wireless LAN. Since NYI's beacons are radiating out onto the street by remove the SSIDs from the beacon frames can help in "hiding" their radio network from war drivers and war chalkers.

SSID filtering is not considered a total security solution in and of itself but used with other methods helps securing the wireless infrastructure.

MAC address filtering.

There are several methods that MAC address filtering can be used in a wireless security solution:

Filtering MAC address of only allowed wireless cards in the AP. This ensures that only the wireless cards distributed to employees with the correct MAC address are allowed to associate and authenticate with the AP.

Filtering traffic on the AP downstream Ethernet switch port by using IEEE 802.1X port security. Traffic can be managed at the next hop switch from the AP using 802.1X port security protocols and secure servers such as Cisco Secure ACS, Entrust or any other type of Radius or Tacacs server. The use of Enhance Authentication Protocol (EAP) or Cisco's Lightweight Authentication Protocol for the switch ports connected to the AP can be implemented to control and restrict access from the wireless LAN to the wired LAN in an centralized and efficient manner.

The 802.1x standard provides specifications for port based network access control. Port based access control was originally and still is used with Ethernet switches. When a user attempts to connect to the Ethernet port, the port then places the user's connection in blocked mode awaiting verification of he user's identity with a backend authentication system. EAP which was first defined for PPP is a protocol negotiating an authentication method.

The protocol to be used MD5 TLS GSM OTP etc support of key generation and support of mutual authentication., There are perhaps a dozen types of EAP currently on the market. The successful 802.1x and EAP/LEAP implementation may go as follows:

1. **The client requests association with the access point**
2. **The access point replies to the association request with an EAP/LEAP request**
3. **The client sends an EAP/LEAP identity response to the AP**
4. **The client's EAP/LEAP identity response is forwarded to the authentications server**
5. **The authentication server sends an authorization request to the AP**
6. **The access point forwards the authorization request to the client**
7. **The client sends the EAP/LEAP authorization response to the AP**
8. **The AP forwards the EAP authorization response to the authentication server(like a Cisco Secure ACS, Entrust etc)**
9. **The authentication server sends an EAP/LEAP success message to the AP**
10. **The AP forwards the EAP/LEAP success message to the client and places the client's port in forward mode.**

When 802.1x with EAP is used, a situation arises for an administrator in which it is possible to have a double login when powering up a notebook computer that is attached wirelessly and logging into a domain or directory service. The reason for the possible double login is that 802.1x requires authentication in order to provide layer 2 connectivity. In most cases, this authentication is done via a centralized user database. If this database is not the same database used for client authentication into the network (such as a Windows domain controllers, Active Directory, LDAP or NDS), or at least synchronized with the database used for client authentication, then the user will experience two logons each time network connectivity is required.

Timed based filters can also be applied in combination with the solutions above to further restrict the use access of the wireless network from someone using a spoofed address after hours across the street.

Although MAC filters may seem to be a good method of securing a wireless LAN in some instances, they still susceptible to the following intrusions:

Theft of a PC or card that is in the MAC filter list of an APA(an immediate change process should be able to mitigate this issue)

Sniffing the wireless LAN and then spoofing with the MAC address after business hours. See the timed based filters above. Some wireless Pc cards permit the changing of their MAC address through software or even operating system configuration changes. Once a hacker has a list of allowed MAC addresses the hacker can simply change the PC card's MAC address to match one of the allowed pc cards on the wireless network, instantly gaining access to your entire wireless LAN.

Layer 3-7 protocol filtering.

Wireless LANs can filter packets traversing the network based on layer 2-7 protocols. In many cases, manufactures make protocol filters independently configurable for both the wired segment and wireless segment of the AP.

Filters for just SMTP, HTTP, certain broadcasts et. al. will ensure only a certain type of traffic and to a more important extent only certain type of existing or future exploit will be allowed into the network thus making it easier to identify the class and signature of any type of intrusion.

Remember that WEP protects only layer 3-7 information and data payload , but does not encrypt MAC address or beacons.

Wireless VPN

Wireless LAN manufactures are increasingly including VPN server software in access points and gateways, allowing VPN technology to help secure wireless LAN connections. When the VPN server is built into the access point, clients use off the shelf VPN software using protocols such as PPTP or IPsec to form a tunnel directly with the access point.

Use of PPTP with shared secrets is very simple to implement and provides a reasonable level of security, especially when added to WEP encryption. Use of IPsec with shared secrets or certificates is generally the solution of choice among security professionals based on AMI's experience. Manufactures offer many features to make wireless VPNs easier and economical to implement. A review of NYI's wireless equipment manufacture's offerings on VPNs should be considered.

Turning off DHCP for wireless devices

Depending on the tradeoff of ease of use and security this option should be considered. If the AP or a local DHCP server is providing IP address once the network is compromised it now becomes very easy for a hacker to have a valid address assigned thus making it easer to roam the network. By turning off this feature would make the hackers life a little more difficult for extra time is required to sniff and scan for address and subnet info to use plus discover DNS and Default Gateway devices. This action alone could deter the casual war driver for it is too much effort and he/she will move to easier targets. Of course the down side is manual address assignments for the wireless clients and administration.

Wireless gateways

Enterprise wireless gateways are a special adaptation of a VPN and authentication server for wireless networks. An enterprise gate sits on the wired network segment between the APs and the wired upstream network. As its name suggests, a gateway controls access form the wireless LAN on the wired network, so that, whole a hacker could possibly listen to or even gain access to the wireless segment, the gateway protects the wired distribution system from attack.

Another use is to move the AP wired section to the DMZ so all wireless users will go through the same "front door" to the corporate resources just as other VPN or internet users do. This could also be accomplished by using a separate VLAN for the APs that can be deposited onto the DMZ. The use of the VLAN secures the wireless traffic as it traverses the wired corporate network. See the recent Cisco announcement of its products supporting VLANs below for more information:

Cisco Wireless LAN Software Center - UPDATE:

Cisco Aironet Products Support Virtual LANs and Quality of Service

The waiting is over! Now you can take advantage of the flexibility of virtual LANs (VLANs) and the hands-on control of quality of service (QoS) in your wireless network. Cisco Aironet firmware version 12.00T supports VLANs and QoS on Cisco Aironet 1200, 350, and 340 Series access points and the Aironet 350 Series Wireless Bridge. In addition to VLANs and QoS, version 12.00T also supports:

- **Multiple service set identifiers (SSIDs)**
- **Centralized administrator authentication**
- **Improved handling of lost Ethernet connectivity**
- **Secure shell support for secure Telnet interfaces**
- **Reporting on access points that fail authentication with LEAP**

Download Cisco Aironet firmware version 12.00T today from the Cisco Wireless LAN Software Center, with the step-by-step Aironet Wireless Software Selector or the Software Display Tables:

www.cisco.com/tac/newsletter/0103_wireless_lan_software.html

Using a central authentication system as discussed earlier to enhance the security of the Authentication and Association process. By having the Open System Authentication or the Shared Key Authentication process which ever is used by NYI authenticate to a backend server help in the administration and securing of the this critical process.

The use of a separate Wireless DMZ

Create a separate DMZ for wireless users to enter the corporate infrastructure using some of the methods listed earlier such as a VLAN for wireless traffic from AP to the DMZ and wireless gateways and firewalls to log and control traffic allowed from the wireless segments to the corporate segments.

Lost or Stolen wireless devices

A process to quickly handle the loss of wireless cards and laptops should be defined if not already. These lost devices have the WEP key embedded and can be used to gain access to the network easily. A process to change WEP keys, MAC filters etc. should be put into place so there is a short, if not, no window of opportunity for the hacker to use the lost/stolen equipment.

Physical security

In order to reduce the chance of eavesdropping, NYI should make sure that the cell sizes of access points are appropriate. The majority of hackers look for the locations where very little time and energy must be spent gaining access into the network. According to Figure(1 and 7) NYI is inadvertently making it easy for the hacker or casual eavesdropper. For this reason, it is important to not have access points emitting strong signals that extend out into a parking lot, street or even a neighboring building. Some enterprise level APs allow for the configuration of power output, which effectively controls the size of the RF cell around the access point. If the cell size is reduced to the point that the hacker cannot even see the network from the parking lot, street or next door your network will not likely be attacked from this point. This was mentioned earlier in the AP association/authentication process discussion in this report.

Radio frequency/cell size management

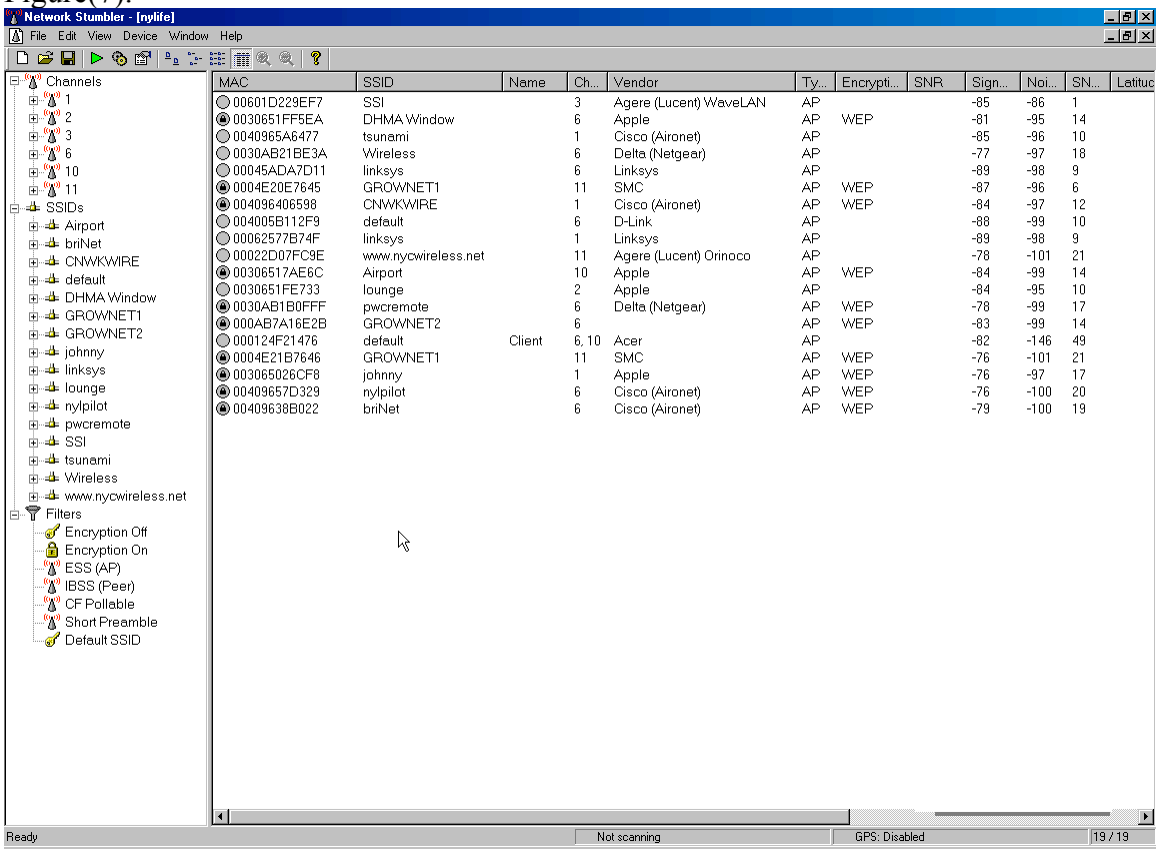
In NYI's case the cell sizes of the channels used is seen easily from street level and possibly down several blocks. This is because of the wattage/dBm output, antenna polarity, placement of APs and types of antennas used. NYI should consider looking into changing the polarity and direction of the beamwidths of APs to the point that the RF cells originate from the perimeter of the building inward thus reducing any RF signals sent to the street due to the diversity antennas. Some recommendations in regards to cell size management:

1. The use of RF attenuators to reduce the Cell size, not recommended, only in an extreme case.
2. The use of sectional, directional or omni-directional antennas to focus the beamwidth within the building and away from the street.
3. Reducing the power output of the AP to thus shrink the cell size within the building.
4. Change the auto rate adjustment feature if applicable in the APs.

Access Point Audits

NYI should conduct periodic security audits for rogue APs. By using the same tools that hackers use and the ones listed and used to create this report, NYI can conduct periodic RF sweeps to ensure that no additional non authorized APs have been added (with or without WEP enabled) to defeat NYI's wireless security efforts. As per Figure(7) there are other APs listed that may or may not belong to NYI. NYI should investigate to ensure that these APs are not active in their building. Notice that these other questionable APs do not have WEP enable thus making it easy for anyone from the street to access NYI's network if they are NYI APs. The list of APs in Figure(7) shows many different AP with names that may or may not be relevant to NYI and some of them doe not have WEP TURNED ON.

Figure(7).



AMI can demonstrate the tools used to conduct such an audit.

Corporate security policy

A company that uses wireless LANs should have a corporate security policy that addresses the unique risks that wireless LANs introduce to the network. The example of an inappropriate cell size that allows the drive by hacker to gain network access from the parking lot or across the street is a very good example of one item that should be included in any corporate security policy. Other items that should be covered in the security policy are strong passwords, strong WEP keys, physical and RF security, use of advanced security solutions and regular wireless LAN hardware inventories(periodic scans for rogue access points) will help in further securing the wireless network.

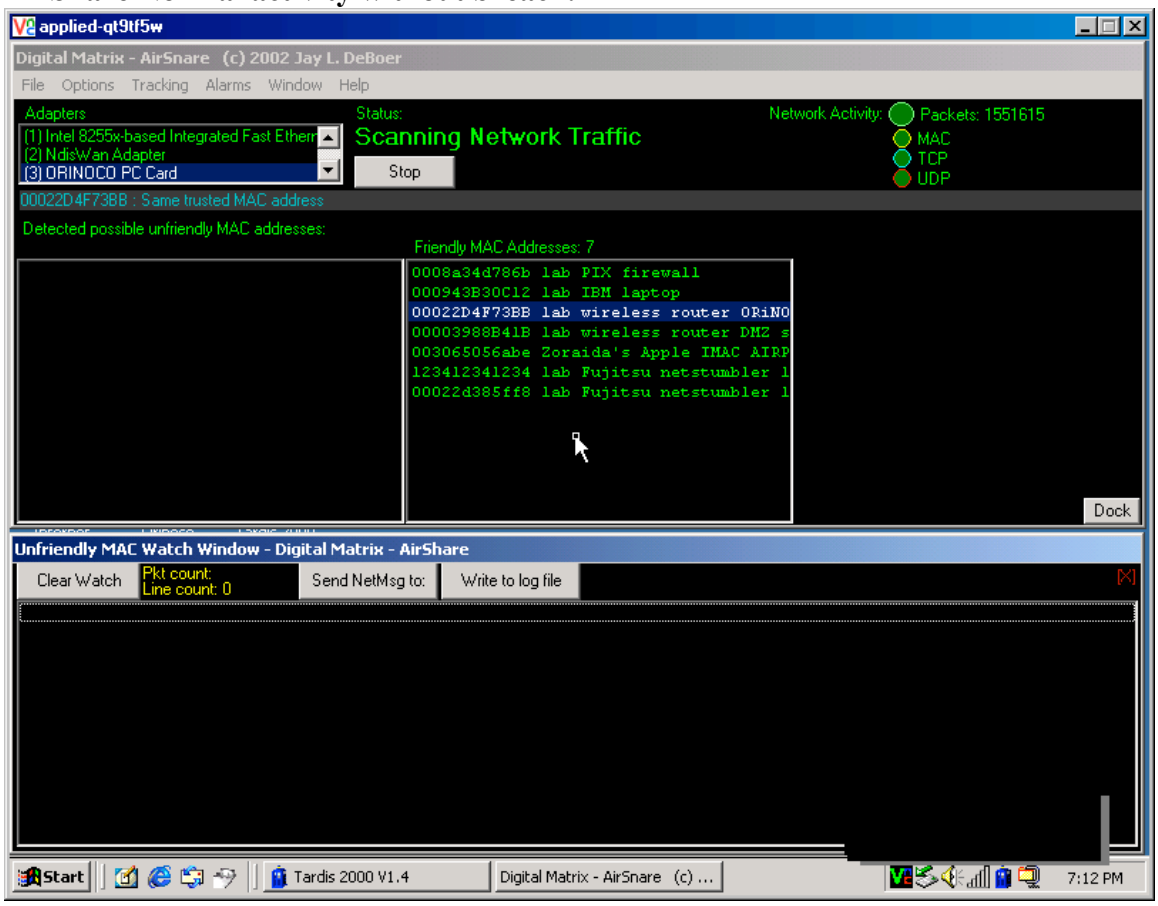
Wireless Intrusions detection tools

AMI has been actively researching and beta testing several wireless security tools some shareware and other commercial that provide a basic intrusion detection system to identify and deter possible war drivers, hackers and other probing activity conducted on your wireless network.

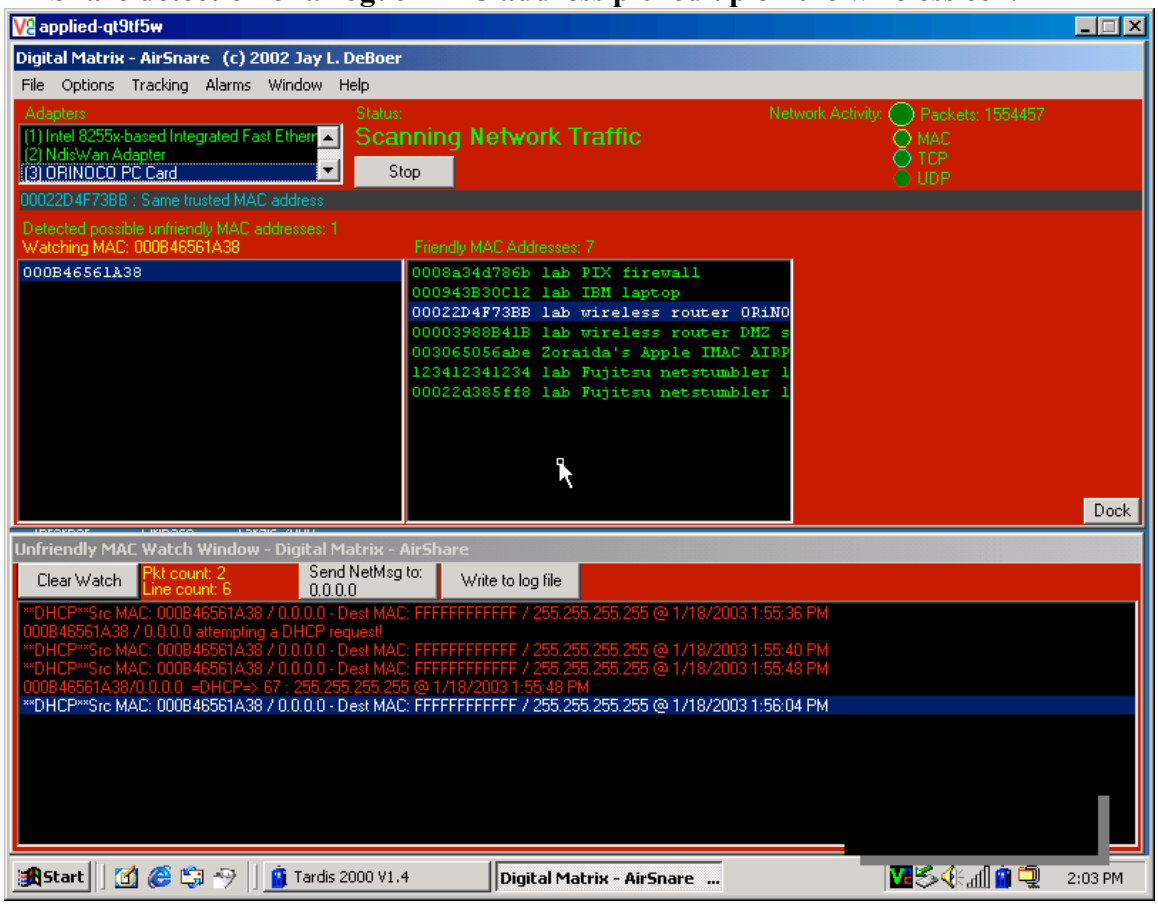
Some of these solutions are free or very low in cost and can provide an immediate return on investment. Some of the solutions can utilize older hardware that NYI may already have and may discard thus reducing the overall cost of the IDS system. The only cost in one solution is just the 802.11b radio cards.

One such solution that AMI can demonstrate for NYI is AirSnare. AirSnare is a shareware application that detects DCHP requests and un-trusted MAC addresses on a wireless cell. The application can then play a wav file and send an email to the administrator when the intrusion happened. Also AirSnare lets the administrator send a message back to the intruder to get off the network. With older laptops or PCs and the low cost of 802.11b radio cards and remote control software such as VNC NYI can deploy several of these low cost wireless IDS systems on the perimeter of their building for under $100.00 per device. Several screenshots of AirSnare in action are shown below:

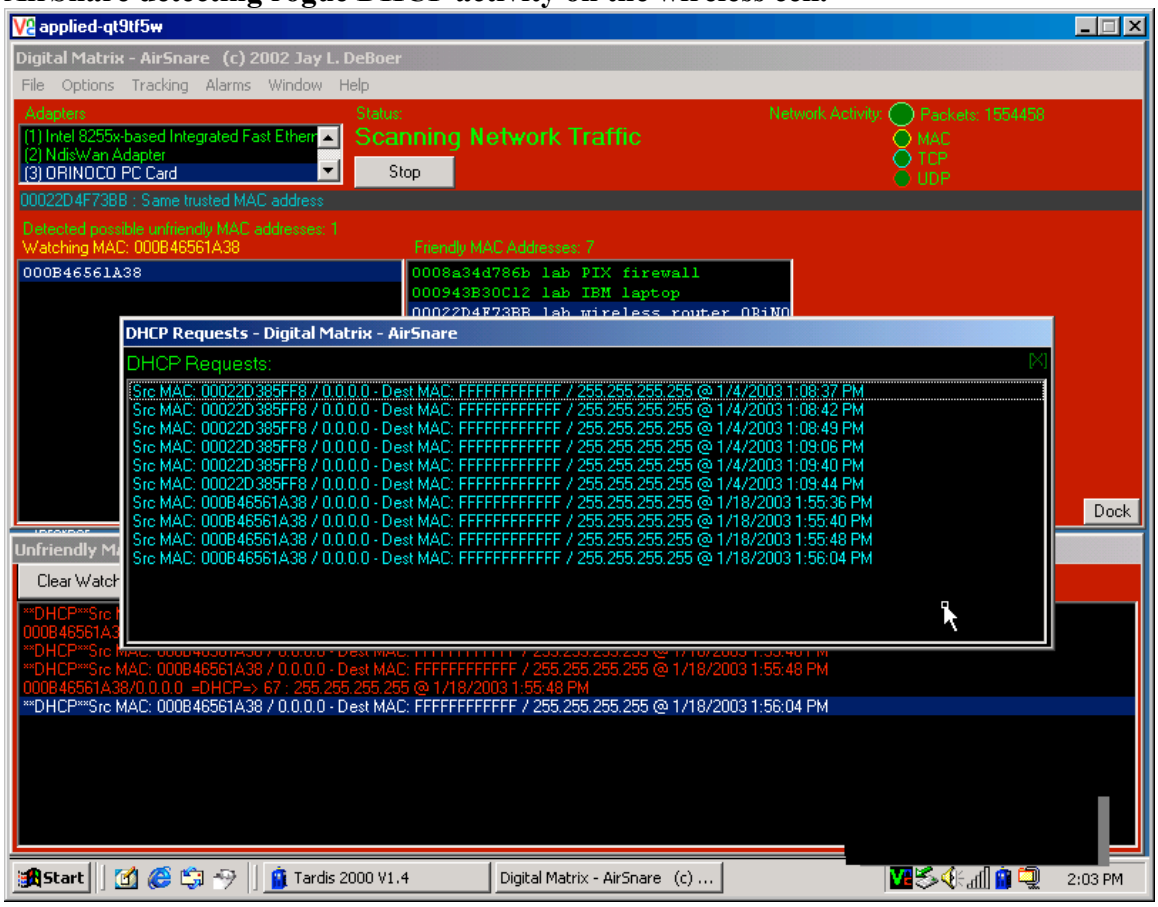
AirSnare Normal activity without breach.



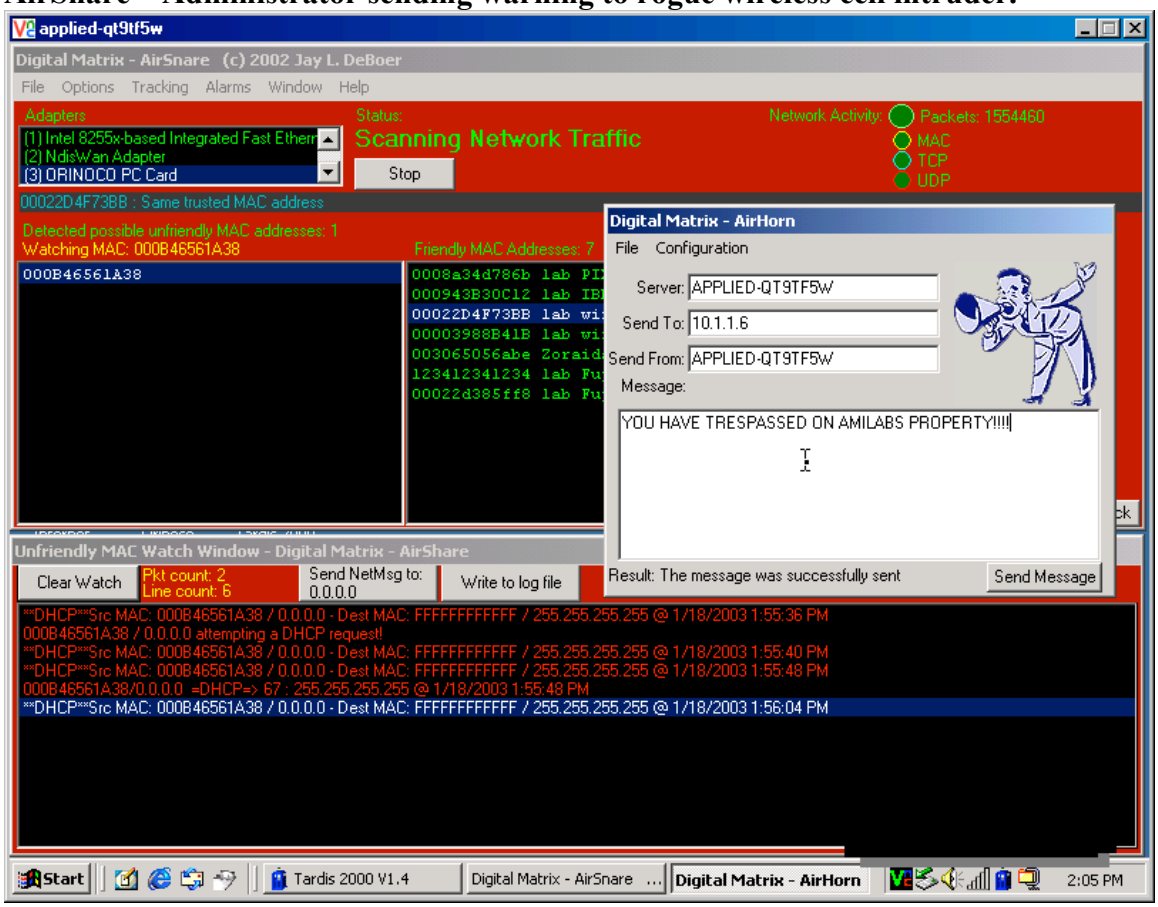
AirSnare detection of a rogue MAC address picked up on the wireless cell.



AirSnare detecting rogue DHCP activity on the wireless cell.



AirSnare – Administrator sending warning to rogue wireless cell intruder.



A sample of the email contents warning the administrator of a rogue MAC address present on the wireless cell is below:

```
AirSnare has detected an unfriendly MAC: 000B46561A38 on the network!
```

Other tools that AMI can demonstrate for NYI are as follows:

- NETSTUMBLER
- AIRSNORT
- WEPCRACK
- KISMET
- AIRMAGNET
- PACKETYZER/WSP100
- LINKFERRET
- NSSPYGLASS
- GETPASS

Summary

AMI has identified a potential and serious weakness in NYI's network infrastructure for if not attended to could lead to serious consequences. One such consequence is the use or destruction of NYI data assets on its computing systems. One such approach is that hackers could gain access to NYI's network via the wireless "backdoor" to wreck havoc on NYI systems thus causing difficulty for NYI to operate and incur severe operating costs to recover. Attacking corporate networks as outlined in the federal government's Critical Infrastructure Protection Board is not a new concern however with the advent of wireless technologies, its ease of use, the tools available and its inherent RF security weakness this concern should be highlighted. AMI hopes the information provided in this report helps NYI mover closer to a more secure network infrastructure. AMI looks forward to discussing such issues outlined in this report at NYI's convenience.