GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

GIAC Certified Incident Handler
GCIH Practical Assignment
Version 2.1.a
Option 1

War Driving Exploits on Wireless Systems

Submitted by

George S. Smith

August 18, 2003

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Executive Summary:

The paper reviews the combined exploits of WiFi war driving and MAC address spoofing to gain access to the system. Opening screens of Windows-based software that can be used in carrying out the exploit are illustrated, i.e., NetStumber, SMAC, and AirSnort. A full explanation of the steps in the attack is provided.

It is assumed, as noted in several WiFi references, the wireless transmissions are unencrypted or at a minimum only WEP encrypted. A variation of the exploit is provided explaining how to overcome WEP encrypted systems.

Incident handling for this exploit is illustrated with the ABC Company case. The ABC Company uncovers an unauthorized WiFi network running on its premises. Company technicians use software that could be used to exploit a system to identify and disconnect the unauthorized system. All parts of incident handling—preparation, identification, containment, eradication, recovery, and lessons learned—are considered under the ABC Company case. The ABC Company is not a "hacker," yet the Company did use NetStumber and MAC addresses to perform a war driving operation on its offices.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table of Contents

Part I: The Exploit

1.1 MAC Address Spoofing 4
1.2 Operating System 4
1.3 Protocols 4
1.4 Brief Description of the Attack 4
1.5 Variants 5
1.6 References 5

Part II: The Attack

2.1 Describe and Diagram the Attack 6
2.2 Protocol Description 11
2.3 How the Exploit Works 13
2.4 Describe and Diagram the Attack 14
2.5 Signature of the Attack 15
2.6 How to Protect Against the Attack 15

Part III: Incident Handling Process: The ABC Company

3.1 Preparation 17
3.2 Identification 18
3.3 Containment 20
3.4 Eradication 21
3.5 Recovery 22
3.6 Lessons Learned 22
3.7 Extras, if any 24

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

WAR DRIVING ATTACKS ON WIRELESS SYSTEM:
(Version 2.1a)

Part I. **THE EXPLOIT**:

1.1 MAC Address Spoofing:
The paper analyzes the methods that can be used to combine war driving with MAC spoofing to gain unauthorized entry into wireless (WiFi) networks.

1.2 Operating Systems:

1. General Operating systems:
Windows OS and 801.11 wireless fidelity (Wi-Fi) radio signals for "smaller" network.

2.4GHz for 802.11b
5 GHz for 802.11a

2. Operating systems for NetStumber and SMAC 1.1*. SMAC is specifically designed for Windows 2000 and Windows XP.
Windows 2000*
Windows 98
Windows 95
Windows Me
Windows XP*

3. WiFi Orinoco Min Card (PCI card)

4. Linksys AP configuration:

a. SSID and MAC used as identifiers
b. WEP used as the encryption method.

1.3 Protocols

HTTP protocol
802.11 a and 802.11b wireless systems
WEP 40-bit key encryption
NdisReadNetworkAddress protocol

1.4 Brief Description of the attack:

A war driving exploit using spoofed MAC addresses is being examined here. War driving is the opening step in an exploit that is used to gain unauthorized access to wireless systems. The war-driving exploit involves several steps that must be separately carried out to gain unauthorized access to a network. In this paper, these steps will be viewed as (1) identification of the wireless signal and the (2) sniffing, possibly decrypting, and spoofing of authorized IDs to gain

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

access. The following quote shows why adding encryption on wireless chips does not complicate the exploit over not having any encryption.

> "The Orinoco RG-1000 residential gateway ships by default with Wired Equivalent Privacy (WEP) enabled. Unfortunately, the default WEP key is set to the default network name, SSID. The SSID appears in several 802.11 management frames in the clear-- even when WEP is enabled. Therefore, an attacker with a sniffer capable of capturing management frames can determine the current WEP key which is the last five digits of the network name, (provided the default has not been changed). Armed with the network name, and the current WEP key the attacker can easily gain access to the users wireless LAN. Additionally, the default network name for the unit studied was the last six nibbles of the AC address converted into ASCII [1]. As a result even if the key were not the network name, an attacker could determine it by sniffing the MAC address of the unit. To Lucent/Ornioco's credit, the fact that the default encryption key should be changed is strongly encouraged in the manual. However, the fact that the default key is disclosed in the clear as part of the network name is unfortunate. The default encryption key should be changed to a randomly generated value set at the factory."
> http://archives.neohapsis.com/archives/bugtraq/2001-04/0020.html

1.5 Variants:

A check of the Common Vulnerabilities and Exposures site (http://www.cve.mitre.org) resulted in the following exploits as "candidates" for inclusion in the paper. Reviewing the cert.org site did not find any similar wireless exploits.

1. CAN-2001-0618 (under review). Orinoco RG-1000 wireless Residential Gateway uses the last 5 digits of the 'Network Name' or SSID as the default Wired Equivalent Privacy (WEP) encryption key. Since the SSID occurs in the clear during communications, a remote attacker could discover the WEP key and decrypt RG-1000 traffic. http://www.cve.mitre.org/cgi-bin/cvekey.cgi?keyword=802.11

2. CAN-2001-0619 (under review). The Lucent Closed Network protocol can allow remote attackers to join Closed Network networks that they do not have access to. The 'Network Name' or SSID, which is used as a shared secret to join the network, is broadcast in the clear. http://www.cve.mitre.org/cgi-bin/cvekey.cgi?keyword=802.11

1.6 References:

1. Dell Technology White Paper: Wireless Security in 802.11 (Wi-Fi®) Networks. January 2003.
http://www.dell.com/downloads/global/vectors/wireless_security.pdf
2. Jeff Duntemann's Wardriving FAQ. April 26, 2003.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3. MSDN: NdisReadNetworkAddress. June 05, 2003. http://www.msdn.microsoft.com/library/default.asp?url=library/en-us/network/hh/network/103ndisx_9omsq.asp
4. NetStumber.com. Software download of NetStumber and ReadMe instructions. http://www.netstumber.com.
5. SMAC 1.1 Release Notes: http://www.klcconsulting.net/default.htm?v=readme11
6. Bob Mims. Hunting for Hot Spots. *The Salt Lake Tribune*. June 29, 2003. http://www.sltrib.com
7. Erik Sherman. Walk-by-Hacking. *The New York Times Magazine*. July 13, 2003. http://www.nytimes.com/pages/magazine
8. How Does a Wireless System Work? A Technical Look At Wireless Communication. http://www.rversonline.org/WiFi.html
9. Air Defense White Paper. Wireless LAN Security: What Hackers Know that You Don't. 2003. http://www.airdefense.net
10. Joshua Wright. Detecting Wireless LAN MAC Spoofing. January 21, 2003. http://home.jwu.edu.jwright
11. William A. Arbaugh, Narendar Shankar, and Y.C. Justin Wan. Your 802.11 Wireless Network has No Clothes. March 30, 2001. www.cs.umd.edu/~waa/wireless.pdf
12.Dell Technology White Paper: Wireless Security in 802.11 (WiFi) Networks. January 2003. http://www.dell.com/downloads/global/vectors/wireless_security.pdf.

Part II. THE ATTACK

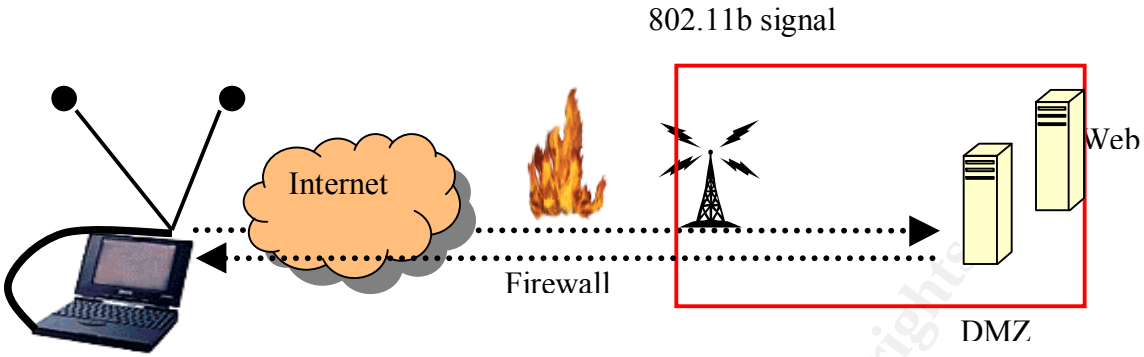
The MAC attack is being launched against a wireless site that uses a Windows operating system and Windows attack software. It is assumed the MAC and SSID addresses are not encrypted.

2.1 Describe and Diagram the Attack

The WiFi wireless network diagram follows. It is set up as an infrastructure model. In the infrastructure model, all clients send their communications to one point…. the access point (AP). The AP is shown as a tower in the diagram. The AP resends the incoming communication to the wired network or other wireless systems with an internal corporate network, for example. The infrastructure model is in contrast with an ad hoc network. Another alternative is the ad hoc network that is similar to a home network whereby each of the wireless PCs would communicate with one another but one PC would be required to act as a "server" to the external network.

Wireless networks can be set up as open or closed networks. An open network is available for anyone to use whereas a closed network requires the user know the SSID (network name) and other password to join the network. Also, a network may control access based on the MAC address of connecting PC.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



War Driving Example:  (using a car the speed should be about 35 mph)

Step 1 or finding the signal: The notebook is equipped with a WiFi Orinoco Min Card (PCI card) and placed inside a car. The PCI card is not built into the notebook but instead it is an external card. A directional antenna is connected to the PIC card with a pigtail (RMC connector). The purpose of the antenna is to identify a signal coming out from a firewall protected wireless network. The antenna can be homemade or purchased from various vendors. The cable from the NIC card to the antenna is called a pigtail, and it connects to the antenna with a normal coaxial connection and an RMC connector to the PCI card. If the PCI card's antenna is built into the notebook, it may be necessary to hack the card by opening the notebook to connect an external antenna. External antennas have better wireless reception than built-in antennas. The other more sane choice is to buy a second card with an external antenna connection for the notebook.

Equipment requirements:
1. Notebook with External PCI Card, Orinoco Gold Card.
2. An external antenna for better reception.
3. A pigtail between the 5dBi omni directional antenna (car roof mounted) and the notebook.
4. It is also possible to identify wireless signal using a WiFi Finder available from PC Mall for $24.95. This signal finder works without being connected to a PC. It is used to discover if 802.11 signals are present. After which, the notebook can be turned on to begin identifying the signal.

Once the external antenna is connected to the notebook, it will necessary to use NetStumber to identify SSID and MAC data about the wireless transmission coming through the firewall

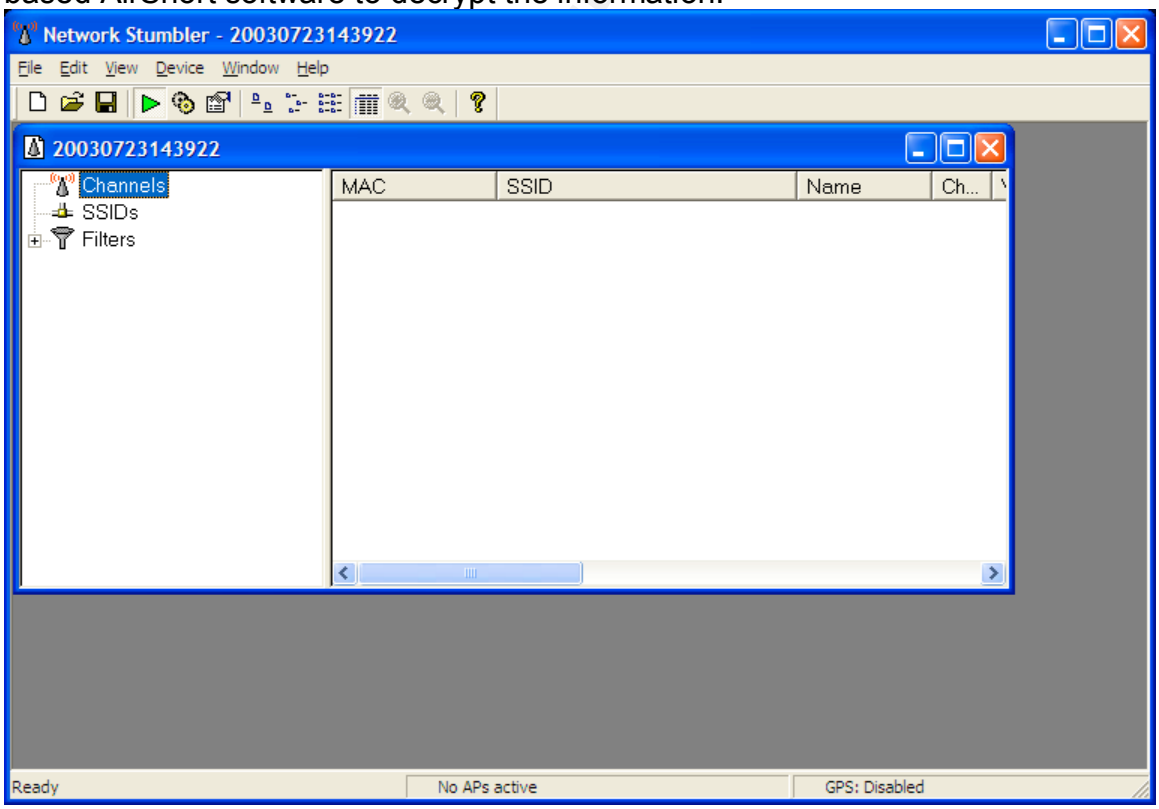
Step 2 or reading the signal: NetStumber is the free software used to identify wireless signals once the notebook's antenna has been deployed. The software

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

package analyzes 802.11 headers to determine service set identifier (SSID), media access control (MAC) address, wired equivalent privacy (WEP) packet usage, WEP key length (40 to 128), signal range and the access point vendor. SSID is a wireless domain name and MAC is an identifier for a specific PC on a LAN. NetStumber works with Windows operating systems (OS), but it does not provide for the unauthorized access to a wireless network using an 802.11b signal. NetStumber 0.3.30 supports an Orinoco Cards, i.e., Hermes chipset. The 0.3.30 version may work with Prism chipsets.

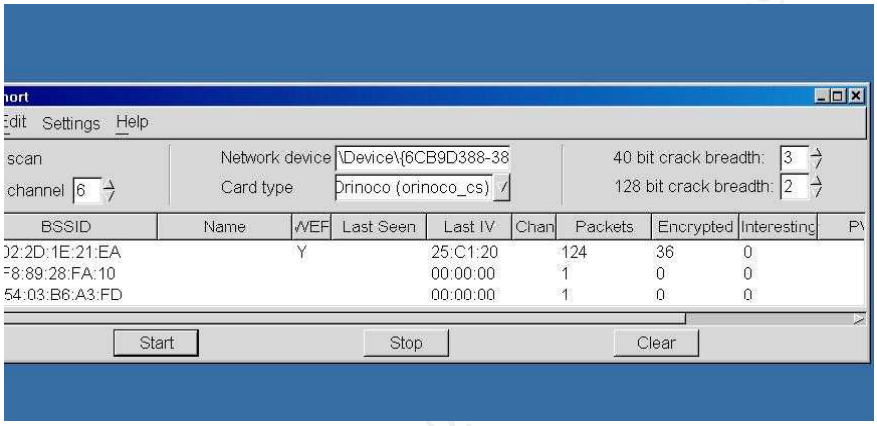
NetStumber works by sending a probe request (similar to a network ping) to all wireless access points within the antenna's range. Thus, an external antenna expands the range. The following screen shows the opening screen for NetStumber. The lower portion of the screen shows that no APs are active and that GPS is disable. AP can be viewed as a device that sends data between networks, i.e., in this case between a wireless and wired network.

If the AP beacon is disabled, NetStumber will not detect the signal. It is possible to use GPS with NetStumber to plot the location of access points on area maps. The filters button allows for sorting signals by various criteria such as WEP usage. In the screen shot, it can be seen the MAC and SSID addresses will be shown. If these addresses are encrypted, it will be necessary to use Windows-based AirSnort software to decrypt the information.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Step 3 or beating encryption: Once NetStumber has identified a wireless signal; the next step is to gain access to the network. If the system is open, i.e., using MAC or SSID as passwords, network access is gained at this point. NetStumber will signal with a padlock icon when WEP encryption is being used. If the system is WEP encrypted, it is necessary to use a packet sniffer to collect wireless packets and then crack the encryption in those packets. In a Windows system, a wireless sniffer is available from AiroPeekNX (http://www.wildpacket.com). This commercial software package costs more than $3,000 to purchase. Another Windows-based sniffer is AirSnort for Windows. The opening screen for this sniffer follows as shown here and at http://airsnort.shmoo.com/AirsnortWin.jpg. Downloading information is available at http://airsnort.shmoo.com/windows.html. Under WEP encryption, clients and APs use the same key to encrypt and decrypt data. In addition, there is no protocol for key management so keys must be manually managed.



Another alternative to Windows-based AirSnort is to use one of the Linux-based sniffers to crack the WEP keys. With Linux, the approach is to use TCPDUMP to collect packet coming off the wireless network and then to use a Linux-based version of AirSnort (http://airsnort.sourceforge.net) to crack the WEP keys. Before attempting this, the PCI card needs to be placed into a promiscuous mode so all wireless traffic will be viewed.

It this exploit, it is being assumed the MAC address is used for entry into the network. Once the address is found, it will be spoofed.

Step 4 or spoofing the MAC: The fourth step in this exploit involves the spoofing of the MAC address. The MAC addresses are unique identifiers used to locate devices on a LAN as well as the authentication for entry into an 802.11 wireless network. Network interface cards have a unique ID “burned” into them, but the “soft” MAC addresses on most devices can be spoofed. There are two ways to hide a MAC address. One is the spoofing of the address, and two is changing the burnt-in MAC address.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

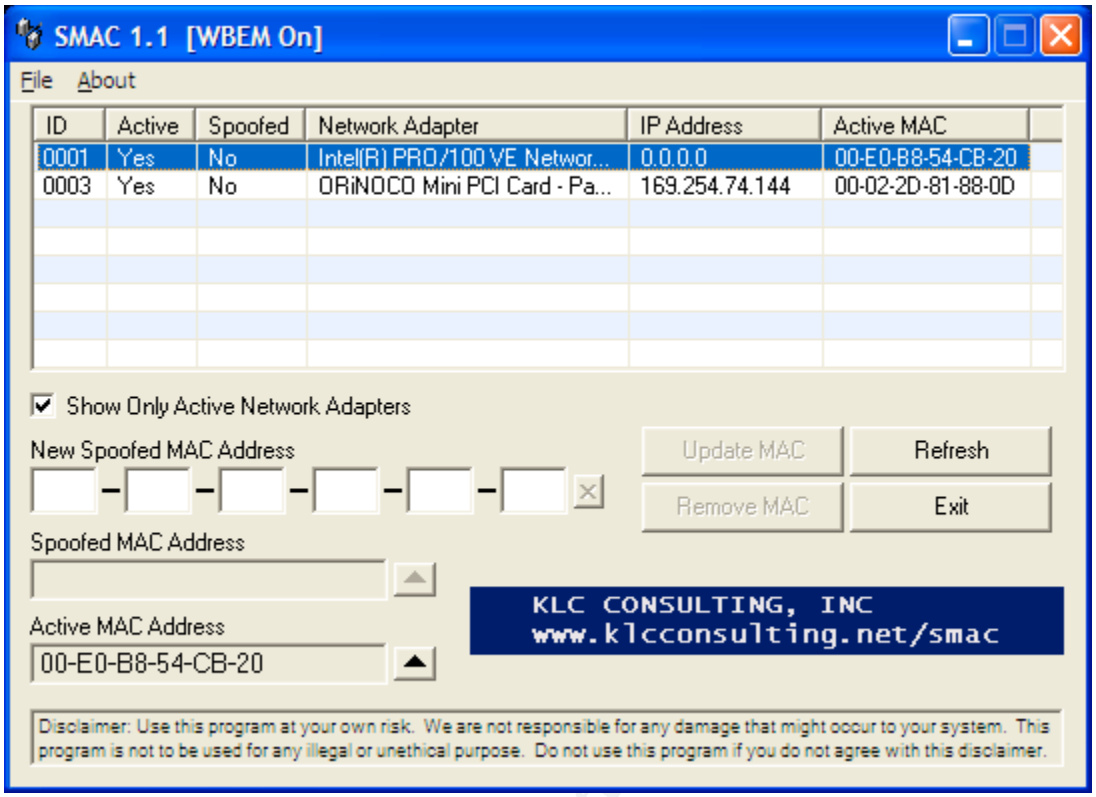
Spoofing is used to disguise the MAC address, but it does not change the burnt-in address on the device. If a wireless network uses MAC addresses to limit access, spoofing an authorized address will allow access past that control as the TCP/IP stack is compromised. Changing the burnt-in NIC address is more difficult as the interworkings of the card's drivers (using IEEE 802.11 standards) must match the MAC address. Thus, trying to change the burnt-in address may destroy the card, as it requires using the card's ports and the I/O address of the chip where the address is written. But spoofing the MAC address without changing the burnt-in address is not as difficult.

Before the techniques of changing a MAC address are covered, it is important to be able to find a MAC address. The procedure for finding a MAC address varies with the operating system. For Windows 95, 98, and ME, click on Start, Run, and type in "winipcfg". The shown adapter address field is the current MAC address. In DOS, type in "NET(leave space)Diag(leave space)/Status" and press "Enter" twice..choose 6 or 7 if requested. Your MAC address is a twelve-digit number. For Windows NT, 2000, or XP, click on Start, Run and enter "cmd" then type in "ipconfig(space)/all and press "enter." Each of these methods should reveal the MAC address on a PC.

The eight-step set of directions for spoofing a MAC address in Windows 98 can be found at: http://www.klcconsulting.net/Change_MAC_w98.htm It must be remembered that with PCs on a LAN, changing a MAC address is likely to make a machine unrecognizable in the network's MAC address list.

Currently, a freely downloadable program called SMAC will allow for changing a MAC address on Windows 2000 & XP systems whether manufacturers allow for this change or not. SMAC 1.1 software is available from: http://www.klcconsulting.net/smac the software requires the user to have full permission to the PC's registry and within a few clicks the MAC address is changed. When changing the MAC address, it is necessary to use the assignments in the IANA Number database (http://www.iana.org/assignments/ethernet-numbers). The initial screen for SMAC follows. It can be seen the software immediately identifies the PCI card type, IP address, and MAC address for the notebook. Also on the screen there is space available to write in a spoof address that has been collected with NetStumber or decrypted with AirSnort. With this simple, change it is possible for the attacker to gain access to the wireless network using a spoofed MAC address. The SMAC program makes use of NdisReadNetworkAddress (NRNA) function in the MS Device Driver Development Kit, i.e. network adapter driver. The driver gets the MAC address in the registry, i.e. the burnt-in MAC address, and then re-programs and overrides the burn-in MAC address.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



2.2 Protocol Description:

Basics. Wireless clients and APs must set up a connection before beginning communications. The concept is similar to the packets sent over the Internet, but the protocols are different. The wireless process begins with setting up an "association" between an Access Point (AP) and the client. The client receives beacon signals sent by the AP. The client receives the beams if the client's antenna is within the range of the AP. These signals allow the client to initially identify the AP. Such signals are likely to contain the SSID identifiers so the client can select among several APs the correct one to select.

Configuring an AP. A web browser can be used to configure the Linksys AP used in a local network by typing in the IP address for the AP within the browser window. The purpose of this first step is to bring up a screen within which to name the AP and to enter its unique SSID number, i.e., the default is "Linksys," into the proper field. It is assumed the network password will not have changed from "admin" during the Linksys' AP setup. In Linksys, a WEP key may be automatically created from the automatically generated passphrase using a hexdecimal mode. The next step is to list the MAC address of those PCs that are allowed access to the AP. These addresses have to be manually entered into the proper Linksys screen. For Linksys, the MAC addresses serve as a filter to the network. The final step is to disable the SSID broadcast from the AP to

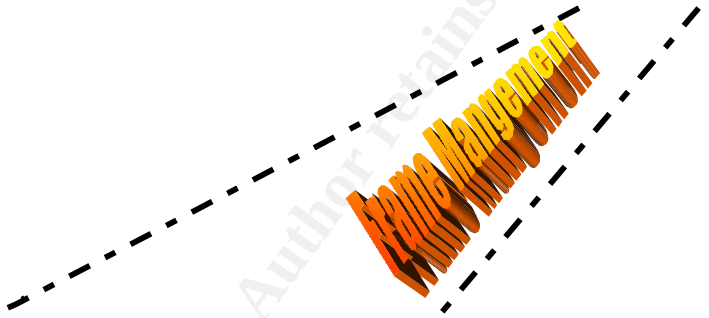
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ensure that NetStumber cannot detect the beacon signal. For this paper, it is assumed that no beacon signals have been disabled.

Using Frames. The client may also send a probe request to a wireless network and find similar identification information in the returning signal. The client and AP then must exchange management frames to begin the association. This is similar to the headers exchanged in the three-step SYN, ACK SYN, and ACK process under TCP/IP connections. Here the association is: unauthenticated/unassociated, authenticated/unassociated, and authenticated/associated.

The frames are illustrated in the following figure for shared-key WEP encryption.

Frame Control	Duration	Des. Address	Source Address	BSSID	Seq. No.	Frame Body	FCS



Algo. No.	Seq. No.	Status Code	Element ID	Length	Challenge Text

WEP Encryption. WEP encryption is centered on the challenge text in the frame and a shared key between the client and the AP. The AP sends a challenge text to the client using a shared encryption key and a randomly generated number. The client responds by re-encrypting the challenge text with the shared key and sending the encrypted message back to the AP for decryption. The AP decrypts the message and ensures the challenge text originally sent is the same as the text received in the just-received frame from the client. If there is a match, the criterion for initial authentication is completed. But, the entire channel authentication is not completed until the AP responds to the client's authentication challenge message in turn. The status code (see frame illustration) will show a zero if the connection has been successful. Otherwise it will contain an error code. The element ID is used to show the frame contains a challenge text. The length field shows the length of the challenge text that can be up to 128 octets. The sequence number can be used as the random number on which the challenge text is based.

WEP encryption standards under 802.11 provide for the use of four-encryption algorithms keys. The AP can decrypt the messages received with any of these

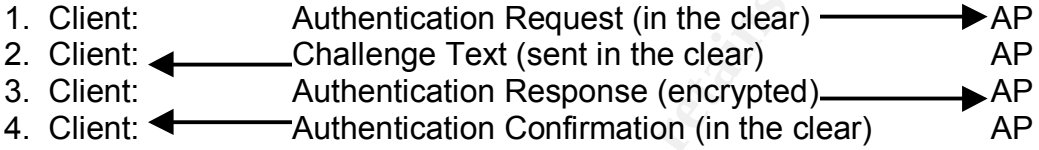
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

keys. Unfortunately, only the default key can be used to send messages thus reducing the difficulty in the unauthorized decryption of the message by a hacker.

2.3 How the Exploit Works

In understanding how the exploit works, it is necessary to understand how frame management works in the wireless network between the client and the AP. The frame management messages sent contain the network name or SSID, and the AP and the client broadcasts these IDs without encryption.

The authentication transmissions occur as shown in the following illustration. The direction of the arrows shows the direction of the flow between the client and the AP. It can be seen that most of the back and forth transmissions occur without encryption.



At this point it is relatively easy for NetStumber to detect the network name or SSID by sniffing the communication authentications protocols. Also, the MAC addresses are shown in the clear. Even in the third step where encryption is used the MAC address are shown in the clear. Once the MAC address is obtained, it is easy to change the MAC address on the attacker's PC to one of the authorized MAC address by using SMAC.

Cracking WEP encrypted messages as currently developed in 802.11 transmissions is relatively easy because of sending clear text messages in the authentication process. By collecting the unencrypted information in the second and encrypted third message, the attacker knows the random challenge (clear text in second message), the shared authentication key, random number generator, and random initialization vector (sent in the clear as part of the challenge text). The third message is sent using the default encryption key. Also aiding the hacker is a protocol that allows all initial authentication communication to be the same, except for the challenge text. With this information, the hacker can reverse engineer the frame body with all the access information and then forge packets to gain access to the network. AirSnort performs this process for the hacker by collecting thousands of encrypted packets from the AP and automatically reverse engineers the information so the attacker can gain access to the system.

Another aspect of the exploit is the NdisReadNetworkAddress. The NdisReadNetworkAddress returns the software-configurable network address, stored in the registry, for an NIC as installed in a machine as shown in the following illustration. SMAC uses NdisReadNetworkAddress protocols to read

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

the MAC address and then the attacker can use SMAC to change the PC's address to a sniffed MAC ID that is used by the network for authentication.

```
VOID

  NdisReadNetworkAddress(

    OUT PNDIS_STATUS   Status,

    OUT PVOID   *NetworkAddress,

    OUT PUINT   NetworkAddressLength,

    IN NDIS_HANDLE   ConfigurationHandle

    );

*Ref:http://msdn.microsoft.com/library
```

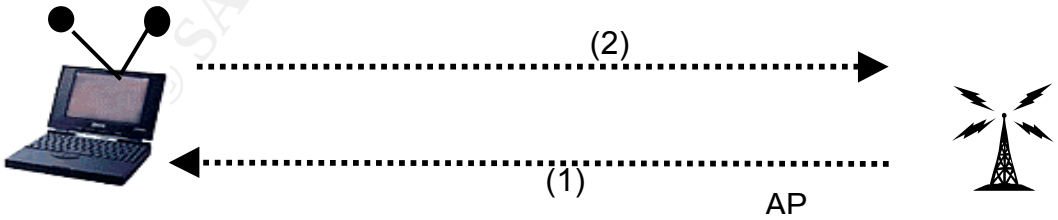
SMAC takes advantage of NdisReadNetworkAddress to find the installed MAC address.

2.4 Describe and Diagram the Attack:

The Unencrypted Attack: The nature of the attack depends on the signal that is being sent from the AP. If the signal is sent in the clear the diagram of the attack is simply the attacker using NetStumber to detect the SSID or MAC address in the beacon and then simply using the SSID or spoofing the MAC address with SMAC to enter the wireless network. The diagram for such an attack follows.



Attacker collects SSID and MAC addresses (s) and enters network using the collected IDs after changing the registry on his or her machine (2).

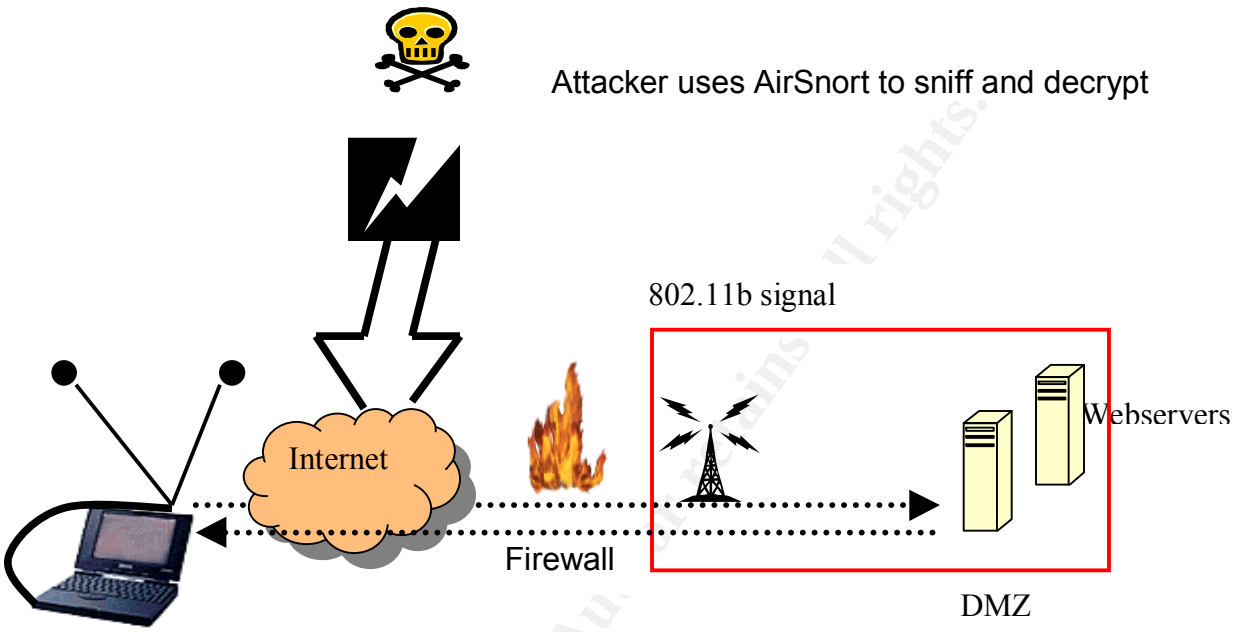


802.11 Signal Beacon:
Broadcasts in the clear

The Encrypted Attack. The following illustration shows the attacker is sniffing the wireless signals going to an authorized user of the wireless network. The

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

attacker is using a sniffer like AirSnort to analyze the communications and break the SSID or MAC identifiers encrypted in the signal. Once the IDs are known, the attacker uses SSID and the spoofed MAC address along with WEP encryption to communicate with the AP.



2.5 Signatures of the Attack

The major signature of this attack is that more than one user is using the access ID to gain to entry the wireless network at the same time. This is a signal that a MAC address, for example, has been spoofed.

In addition, MAC addresses that are out of alignment with the manufacturer's codes would provide an indication of a sloppy attacker as a well-executed exploit would know and use the proper manufacturer's codes.

2.6 How to Protect Against the Attack

Using properly deployed IDS to monitor the wireless system for dual MAC addresses using the network at the same time. The hacker probably spoofs one of these MAC addresses.

Disable the broadcast probe response request from the AP. Without the probe response, NetStumber cannot detect the AP. Although this will not make it impossible for the attacker to find the AP, it will make it more difficult.

Do not use SSID and MAC identifiers as filtering IDs or passwords to enter the WiFi network. The attacker easily identifies SSID names and MAC addresses.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The system administrator prior to going active on the system should change all default identifiers.

Use encryption other than WEP to encrypt the data flowing on the wireless network. WEP can be cracked without too much difficulty therefore stronger encryption should be used in the network to encrypt data flows into and out of the network.

Checks need to be made for "bleeding" of the wireless signal outside the authorized premises. NetStumber is a tool that can be used in the search for wireless signals that are extending beyond the official premises of an organization's physical structure.

Checks should be made to find out if there are unofficial wireless networks being used by employees to communicate with one another both inside the organization's official physical premises. Employees can be using these unofficial sites to communicate between buildings both off and on the organization's physical site. Such networks can have protocols that allow attackers easy access to the organization's entire network. Therefore, these networks need to be closed or brought into the organization's "protected" network.

As with every system, the systems administrator should ensure that all current patches for the specific software are up-to-date and correctly installed.

Use a VPN server for VPN authentication and access to the wireless system. The VPN server isolates and connects the client to the system's internal network, but it does all the work of the authenticating the client thus canceling the need for SSID and MAC filtering.

Review the changes that are taking place in 802.11i protocol for wireless networks. The 802.11i protocol is attempting to overcome the weakness in WEP encryption.

Review the systems that are being developed for encryption key certifications on wireless networks to see if they will work.

Part III. INCIDENT HANDLING PROCESS: War Driving on an Unauthorized System

ABC Company Case: The incident handling process is being developed for a "small to medium" sized company that has just recently installed a new WiFi network for its employees to use. In the past, the ABC Company only had used a hardwired network in its headquarters building. The WiFi system is designed for use inside a building that was recently purchased as part of an expansion in the company's business operations. The lightly remodeled building was

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

originally built in the 1960s, and it was less expensive to install a WiFi network rather than attempt to run wire for a hardwired network. The remodeled building is directly across the street from the ABC Company's headquarters. Although the Engineering Department remained in the headquarters building, the Design Department was moved across street to the newly purchased building. The policy guidelines for network use had not yet been revised to reflect the changes for the WiFi addition.

3.1. Preparation: Acting before the Incident has occurred

Policy: The ABC Company's policy guidelines for network use need to be immediately reviewed. The wireless network has characteristics that are different from a hardwired network and these differences need to be incorporated into the company's network use policies. For example, the number of APs that are used and who has the right to set up these access points as well as their range needs to be quickly determined and codified under network policy guidelines.

Technical security skills: The ABC company needs to start a program to upgrade the skills of every person who has responsibility for securing the wireless system from attack. These skills need to be specifically focused on eliminating the holes in wireless systems. Therefore, even if the company has highly skilled network administrators for its hardwired system those antivulnerability skills do not necessarily transfer into eliminating WiFi vulnerabilities without more training.

Warning Banners: Warnings banners on access screens need to be reviewed to find out if the current announcement adequately incorporates the wireless connections or if the banners need to be updated.

Patch Maintenance: As with any system, patch maintenance is vital to ensure the network is not subjected to a successful attack. In this wireless case, this is important as the source for patches on the wireless network are likely to be different from those downloaded on the hardwired network.

General Training and Updating: The ABC company needs have provided an intensive training program on wireless systems for its network employees prior to the installation. These employees need to understand the vital differences between the hardwired network and the wireless network. Such training should involve teams of employees who receive training and then review their procedures to ensure that items in the following list are updated to incorporate the wireless environment.

(a) checklists;
(b) network diagrams;
(c) incident response team members with wireless skills;
(d) IDS software for wireless systems;
(e) higher-level management understanding;
(f) emergency call lists are updated to include wireless experts;

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

(g) reporting form updates;
(h) log reporting incorporates wireless logins and usage; and
(i) the necessary items have been added to the jump bag, such as equipment to set up additional APs.

Secured Communications: If a hacker successfully penetrates a wireless system, it must be assumed the hardwired system has also been breached. Therefore, any communications should not be sent over either system. It must be assumed the communications on all networks are open to the attacker. It is necessary to have a backup system outside the hardwired and wireless networks as a means of communication among members of the team working on eliminating any penetration of the system. Such secured communication links should be based on hardwired phone systems as cell phone communications may have been compromised.

Legal Review: It is important that a full legal review be made of the wireless system. For example, if a hacker sits between the ABC Company headquarters and their remodeled (across the street) building and picks up unauthorized signals or bleeding from the wireless system, has a law been violated? Is such action viewed as pinging a web server, i.e., legally harmless? Are the actions of a hacker in a public street an illegal action under state legislation? If the hacker is only using NetStumber and geographically mapping ABC Company's signal has a crime been committed? All these new aspects of wireless use need to be reviewed by ABC Company's legal counsel. ABC Company needs to know when it should be protecting its wireless signal and when it is useless to do so because it is not a violation of any legal statute.

Law Enforcement Coordination and Review: With the institution of the wireless network, ABC Company needs to meet with their local law enforcement authorities (hopefully a special high tech investigative unit). The purpose of the meeting is twofold. First, to inform the local authorities that they have established a wireless network, and second to be certain the local authorities have the training to understand the differences in the legal issues between a wireless and hardwired network. It would be disheartening for ABC Company to approach local legal authorities with evidence collected from an attack on their wireless system only to find out at that time local law enforcement has no idea of the wireless legal issues nor do they understand the evidence with which they are being presented.

Penetration Testing: Before implementing a wireless system, it should be penetration tested by a tiger team from a consulting group. It is better to have an outside group do the penetration test, as ABC COMPANY's network employees are new to the system and still learning how it works. Bleeding of the wireless signal outside the building should be a particular focus of the tiger team as it performs its tests.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

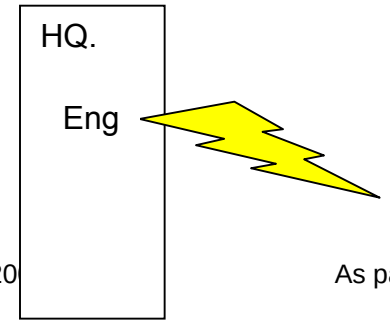
3.2. Identification: Determining whether an Incident has Really Occurred.

ABC Company Case: ABC Company's system administrator John Marsh was taking a break and looking out the fifth story window of the headquarters building on Friday. Traffic was light on the street below, and he noticed Lew Grash from the Engineering Department walking across the street to their newly remodeled building. Lew as carrying his laptop and stopped every few step to type on the laptop. John knew Lew was working on the project with the Designing Department on the Janos project that had to be completed in a little over a week and had the potential to significantly increase sales for ABC Company. John did not give the incident any more thought. Then over the weekend, John realized what he had seen may have been an authorized WiFi network operating in the street between the two buildings. Development Note: The war driving in this case is performed by a legitimate company on an unauthorized wireless network set up on its premises.

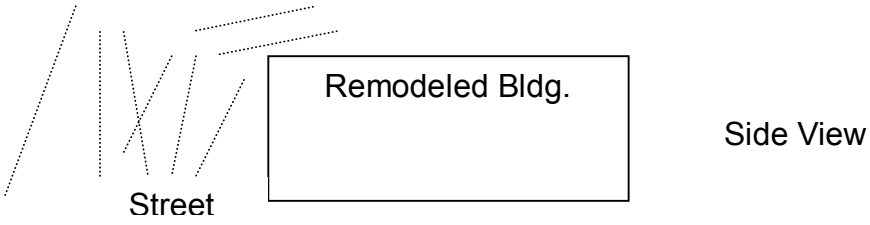
Selecting a Person to Investigate: On Monday, John appointed Jane Landcaster, Assistant Network Manager, to handle the initial investigation and assessment of the potential incident. Jane was instructed to log all steps in her investigation. John felt it was important to find out what was actually going on before confronting any company employee with a charge. At the moment, this appeared to be an internal incident. Any external implications were unclear.

Notifications: John notified the contact list of people in HR, Security, Management, and Legal of the possibility of a potential network incident under investigation. He also indicated the possible results of the investigation were not clear at the present time.

Validate the Potential Incident: Jane began the investigation by running NetStumber to detect any unauthorized APs operating in the headquarters building. She went over the five floors and quickly identified an unauthorized AP in the Engineering Department on the third floor. To better determine the range of the beacon, she walked its path. She determined the signal was largely aimed at the second floor of the remodeled building across the street from headquarters. She also saw the signal was available to anyone in the street between the two buildings. She estimated the range of the signal was 2,100 feet in a direct line between the two buildings and bleeding of the signal resulted in wireless coverage over the entire street area below the signal well as on top of the remodeled building. The wireless network has no encryption and only uses an SSID identifier "Janos" for access. Her preliminary diagram of the signal and its bleeding into the street is shown in the following chart.



© SANS Institute 20 As part of GIAC practical repository. Author retains full rights.



Jane then checked at two web sites (www.wigle.net and www.wfinder.com) to find out if the unauthorized AP's existence has been reported to the world. After checking, she saw that at least it is has not been reported at these two sites.

The conclusion of Jane's investigation is that someone has set up an unauthorized AP and wireless network in the Engineering Department to communicate directly with Designing Department across the street. The signals are the strongest on the in the Engineering Department and in the Design Department. She does not know if the network is connected to ABC Company's hardwired network or whether it has been used as an unauthorized access point for hackers.

Jane's report to John identifies her company authorization to make the report and each of the steps that she has taken along with the date of its occurrence and the results of each step of the analysis. She provides John with a copy of her report.

Identification of an Incident: John decides the information provided by Jane is enough to classify the signal as an incident. In addition, he knows the Janos project is an important project to the ABC Company. Further, the project is facing a tight deadline schedule. He activates the company's incident handling team and notifies Security. A designated person in the management organization chart is also notified.

3.3. Containment: Defining the containment area and limiting damage

ABC Company Case: John is certain that a wireless network has been set up between the Engineering and Designing Department to better coordinate their work and try to meet the deadline for the Janos Project. John knows that a disruption in the work schedule may mean the ABC Company will lose the project and millions of dollars in sales. At the same time, he knows that if the wireless network is connected to the Company's hardwired network, hackers could gain access to the Company's entire network and begin destroying their files. He believes he is a lose-lose situation. The shutting down the unauthorized AP may allow the transfer of blame to his office should the contact deadline be missed. Not shutting down the wireless network could result in the Company's entire network being compromised.

Incident Team Activation: The Incident Team is activated. The small incident team (IT) is trying to keep a low profile in the company and it is documenting its

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

activities using an Incident Survey similar to the one in the back of the booklet *Computer Security: Incident Handling Step by Step* (The SANS Institute, October 2001). The MAC addresses of the devices using the unauthorized AP are being documented in the survey documents. NetStumber is used to collect this information. Additional information is documented as to the number of times and dates that the system is active. Later, this information can be correlated with the work schedules of the suspected employees using the unauthorized network. At the present time, it is uncertain which employees are using the system or who set up the system. The quickest with which the investigation has begun is resulting in IT using NetStumber rather than a commercial software package to collect the data.

IT members want to make a determination if the Company's main hardwired network has been compromised. Network logs from the last two weeks are reviewed as well as system binaries to find out if any anomalies can be spotted. IDS logs are reviewed. The steps are all documented by date, employee doing the analysis, and results. The team determines the network appears secure at this point.

The team estimates the size of the files being transferred between the Engineering and Design Department by the time they take to transfer over the network. It is determined that these files are probably confidential company files, i.e., not personnal, and they are being transferred, in the clear, over the wireless network. Such files would have a market value if obtained by an attacker.

IT is keeping all member of Management, HR, Legal and John aware and briefed about the progress they are making in their analysis as well as the level at which the Company's network policies have been compromised. No attempt has been made to shut the wireless system down or confront anyone running the wireless system.

IT members has ensured that backups of all computer files are now being made on a 5-hour cycle rather than the usual 12-hour cycle. Passwords have been changed, but only if the change would not arouse the suspicions of the employees in Engineering and Design.

IT members have tried to identify the collected MAC addresses that are using the wireless system to a computer. They used the MAC address database at *IEEE OUI and Company_id Assignments* (http://standards.ieee.org/regauth/oui/index.shtml). It is determined that one of the computers is made by Gateway. None of ABC Company's computers are Gateways so it is assumed the network may be based around home laptops that employees are bringing into the Company.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3.4. Eradication: Inadequate eradication can legitimately question the competence of the incident handling team (*Computer Security: Incident Handling*, Sans Institute, p. 28)

ABC Company Case: A meeting of IT members, John Marsh, Management representative, Legal, and HR is convened before any further action is taken. The group is meeting to determine whether the wireless network should be dismantled as it appears to be related to the Janos Project. The effect of not shutting down the unauthorized system is made clear to everyone in the meeting. It is determined the system should be disconnected before the company's entire network is compromised. Legal counsel and HR have provided clearance for Security to work the IT in identifying the AP and the home computers (personal property on Company premises) used to access the wireless network.

Isolate the Source/Cause: It had been determined the AP beacon was not shut off at the end of the workday. Consequently, IT and Security entered the Engineering Department after all the employees had left and identified the location of the AP. They shut it off.

The next morning when Lew Grash tried to turn it on a security video recorded his actions. Security and Legal representative met with him. At first he denied knowing about wireless system, but when confronted with the video he admitted using the system. Eventually, all five users of the wireless system in Engineering and Designing Departments were identified. The employees signed waivers to allow IT to check the MAC addresses on their machines as well as for confidential Company files. The MAC addresses on the personal laptops were correlated with the information collected by NetStumber. It appeared that all the MAC addresses identified on the wireless system had been found. Any confidential files on the home laptops were transferred to Company machines. The engineers and designers admitted to having set up the system so they could efficiently communicated about the Janos Project.

Actions Taken: Legal counsel declined to take any administrative actions against the employees. All five employees were asked to attend three training sessions on the Company's network use policy.

3.5. Recovery: Return the System to Operational Status

ABC Company Case: The employees involved in setting up, using, and running the unauthorized WiFi network initially were not formally disciplined by the ABC Company. Their actions could not be directly related to a violation of a specific paragraph in the Company's network policy use guide. As a result of the disruptions caused by the investigation, the deadline for the Janos Project were not met, and the contract was awarded to another company. Management was aware of this possibility and had accepted it prior to allowing John to make an intervention into the unauthorized wireless system.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Validate the System: IT members proceeded to ensure that no unauthorized wireless systems were set up within the Company premises over the next month with daily overseeing for any new APs. None were found during this period.

Monitoring the System: Both the network logs (the hardwired at HQ and wireless in the remodeled building) continued under close IDS scrutiny during the same period. No unusual activity was detected.

3.6. Lessons Learned: Expansion of Technical Intellectual Capital

ABC Company Case: One week following the shut down of the unauthorized wireless system, IT, Management, and a Security Department representative met with John Marsh to work on an Incident Follow-Up Report. The purpose of the report was to ensure that changes would be made to help prevent employees from developing their own networks in the future.

Monitoring for WiFi Networks: It was decided the procedures for monitoring for unauthorized networks by employees needed to be formalized and strengthen. It was determined that this task with time lines for checking would be added to the system administration dues. Rather than using NetStumber, a commercial package would be purchased.

Use of Home PC: One reason the unauthorized network was successful was because it was based around the home laptops the five employees brought into the workplace and took home with them at night. Management believed that these laptops allowed ABC Company's employees to be more productive. Although Security and IT wanted to restrict employees from bringing these laptops into the workplace, Management vetoed such a policy. Instead, it was decided that all employees carrying laptops off company premises would have them registered and they would periodically be harddrive imaged with follow up checks by Security either as they were brought onto company grounds or removed.

Additional Training: The Report recommended more training for security so they would be able to know how to effectively image a drive and spot check its file architecture.

Software Purchases: The Report recommended the purchase of Encase Software and a review of software available to monitor for unauthorized wireless transmissions. Total recommended purchase cost is $7,500.

Estimated Cost of Remediation: The costs of the investigation and losses were calculated. Personnel costs, i.e., work hours, were an insignificant cost ($15,000) when compared to the dollar value attributed to the lost contract and the potential other loss relationships arising from the Janos Project. It was

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

estimated the lost associated with the incident was $1,200,000. Such costs are related to the lost profits related to probability of winning the Janos Project of $750,000 and the intangible partnering losses arising from losing future business relationships ($455,000). The latter calculation is based on the probability of achieving those future relationships (.70) times the estimated profits arising in the future ($650,000).

Implementation of Actions: The recommendations of the report concluded that Security should be able to begin monitoring laptops within the next 60 days. Although monitoring for wireless networks was currently being done with NetStumber, it was recommended that a commercial package should be up and running within the next two weeks. It was also recommended that monitoring need to be performed both during the workday and in the evening. The Report cited the need for the monitoring to be able to detect APs that are active but have their beacons turned off. At the present time, NetStumber cannot detect an AP if the beacon is turned off.

Review and Completion of the Report: All parties who had helped in the investigating the unauthorized wireless network were sent a copy of the draft report for their comments. After incorporating some added minor changes, the report was completed and sent the ABC Company's CIO.

3.7. Extras, if any

Prologue: As word of the loss to the ABC Company from the employee's actions was circulated, it became clear action need to be taken. The recommendations of the Report were adopted. Eventually, Lew Grash left the ABC Company.

Terminology and Acronyms:

AP (Access Point): a device used to send/receive data between a wired and wireless network.

IT (incident team): The IT abbreviation stands for "incident team."

Locating WiFi Networks: Two web sites provide information about the geographical location of WiFi networks. They are www.wigle.net and www.wfinder.com

MAC (Media Access Control): An electronic address used for locating specific devices (PCs) that are part of a network.

SSID (service set identifier). The SSID acts as a form of password for access to the network. The computer requesting access (client) must present the correct

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

SSID for access to that AP's network. In some cases, the AP will broadcast the SSID.

WAP (Wireless Application Protocol): The protocol used in mobile phones, two-way radios, and pages. These devices are used to connect handheld devices with wireless communications.

WEP (wired equivalent privacy). WEP is a form of wireless encryption of the SSID identifier. WEP is designed to provide a comparable security for a wireless network that is found an enclosed wired network. WEP uses symmetric key encryption algorithm, Ron's Code 4 Pseudo Random Number Generator (RC4 PRNG).

Wi-Fi (wireless fidelity): Radio signal base on 802.11x standards.

WLAN (Wireless Local Area Network): A LAN that uses Wi-Fi radio frequencies to communicate between its connections on the network. It is not hardwired to the PCs on its network.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.