Global Information Assurance Certification Paper

Protecting Your University's WLAN From Rogue Wireless Devices

Sandra D Lindsey

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4c
Option 1

February 08, 2005

1.0 Abstract

Rogue wireless devices have become a serious security threat, particularly across university and college campuses. Since wireless LANs (WLANs) are an open transport technology and do not require physical access, they are already insecure, thus making it more difficult to protect from vulnerabilities caused by rogue wireless devices. This paper is written to give a better understanding of the rogue wireless device issue by defining what is meant by "rogue wireless device," as well as to devise methods for the prevention of such devices, the detection of the devices, and, finally, the remediation for the network once rogue devices have been detected.

The main goal of a secure WLAN is preventing rogue wireless devices from infiltrating the network. If you protect your network by preventing such devices from having access, you will find that detection and remediation are not going to be necessary. However, this is not always possible. Have a plan for detecting rogue devices, as well as a plan for securing the network once the devices have been found.

2.0 Defining Rogue Wireless Devices

A rogue wireless device is considered to be a device that is connected to a private network without the knowledge of the network administrator. Rogue wireless devices can include any number of devices which can be set up by a user who is completely unaware of possible security problems or which can be set up intentionally. The list of possible rogue wireless devices includes, but may not be limited to: an access point (AP) which has been misconfigured; a private AP, which may be either unauthorized or malicious; a personal laptop turned into an AP; a neighbor's legitimate AP; or an ad hoc network.

2.1 Misconfigured APs

A misconfigured AP is a common mistake, yet poses the threat of serious problems for a wireless network. If the AP is not properly configured with the appropriate security settings, the entire WLAN can then be open for anyone who may steal the network's bandwidth or attack the network.

It is possible for an AP to be misconfigured for any number of reasons, with the most obvious being that a novice user just does not understand how to configure the AP. The user will purchase the AP and try to configure it, yet the AP may work fine without the settings being correct. Likewise, the user may set it up using the default settings. It becomes critical that the user understand, although the default settings are a convenience, they are not secure.

Also, take into consideration that there may be several people on a team deploying APs for an entire WLAN. If one of those installers does not

understand the configuration policies and he does not find out what is needed by the WLAN administrator, then the AP(s) installed by that person are likely to be misconfigured. This could mean that sections of campus are completely misconfigured, creating problems for the rest of campus, which is properly configured. It is also important to remember that some APs are set to default to the factory configurations if the AP gets rebooted. Again this leads to the issue that if an AP anywhere on campus is rebooted and the configurations are not carefully checked, the entire network is at risk.

The problem with misconfigured APs is that the AP can, and usually will, continue to function, thus going undetected indefinitely. It is a common assumption that if an AP is working, then it must be configured correctly. However, this is quite the contrary. If even one AP is misconfigured on a Layer 2 network, the whole network becomes vulnerable. Security becomes weak and the service becomes a disaster. It is very important that every member of a wireless project team knows and understands the configuration policies before starting the project.

2.2 Private APs

APs can be divided into two categories: infrastructure or unidentified. Infrastructure APs are purchased by the university and are deployed by members of the WLAN team. Unidentified APs can be private APs, either malicious or no-intent, which are purchased by individuals and are set up without the authorization of the WLAN administrator.

Anyone can go to any local computer or electronics store and buy a private AP. A private AP is generally inexpensive and comes in a variety of speeds and quality. A student may decide that he doesn't want to deal with using the network cable in his dorm room and decides to buy a private AP to plug into the wired network. This one AP is now allowing wireless access for anyone with a wireless card within range of the AP, keeping in mind that the range of an AP can be miles. The student may think he is doing nothing more than creating a convenience, not only for himself, but also for anyone within range. What the student may not realize is that the AP now provides access to hackers who within range of it.

Another problem with private access points is the question of licensed versus unlicensed bands of the radio frequency (RF) spectrum. The Federal Communications Commission (FCC) has regulations regarding the use of unlicensed RF spectrum. The FCC requires that manufacturers of 802.11 products comply with those regulations and must pay to use licensed RF. While unlicensed RF is free, those using it are subject to cause RF interference. Users found to be causing RF interference have no basis for recourse.

The following are just a couple of examples as to when the FCC comes into play

when using private APs:

1. The University of Texas at Dallas (UTD) had been providing wireless access across campus, including student residences. However, some students wanted to pay for access with local ISPs, but decided to use private APs so others could share the access without having to pay for it. UTD said that the private APs interfered with its own network and set policy to prohibit those private APs. The students were outraged that the university would create such a policy and started debates across the country regarding private APs on college campuses. The FCC stepped in and ruled that college campuses can, in fact, prohibit the use of private APs that could interfere with their own wireless networks, but only if the students are trying to put APs in campus housing (or other campus-owned buildings). The problem with UTD was that the student apartments involved were leasing some of the apartments to faculty members. On September 10, 2004, UTD reversed their decision to prohibit the private APs.[1]

2. In 2001, an apartment community in Dallas, Texas, had employed wireless Internet system provider Darwin Networks, Inc., to install wireless access points on the property. The FCC wrote to Darwin to inform the company of complaints of harmful interference to Amateur Radio operations in the area. "Darwin Networks is obligated under Commission rules to locate the source of interference caused by its equipment and make necessary corrections within a reasonable amount of time," said Riley Hollingsworth, FCC Special Counsel for Amateur Radio Enforcement. Because Darwin was not using the appropriate Part 18 Industrial, Scientific, and Medical devices, the company was responsible for resolving amateur complaints, as required by FCC regulations.[2]

Private APs may also be used by hackers for malicious intent. A malicious AP is generally an AP being used by a hacker who is sitting within range of the AP. Once an AP is set up to point to a specific network, it can be used by a hacker to sniff wireless network traffic. The hacker can then collect unencrypted packets to use however he likes.

It becomes critical that users learn to never accept digital certificates without being certain the certificates are valid. Digital certificates enable secure communications across networks. They are issued by a Certification Authority (CA) and validated so the holder's information cannot be forged. The certificate includes such information as the holder's name, the name of the issuing CA, the serial number for the certificate, the start/end dates, and the holder's public key, which is used to encrypt information. Once a user chooses to accept a certificate, he will not see it again until, or unless, the certificate changes. This

creates a problem when an invalid certificate is selected. It also poses the question of whether or not a certificate is needed for each session.

Hackers can use these invalid, or fake, digital certificates to create man in the middle (MITM) attacks by pretending to be the host. When the user chooses to accept the certificate he believes he is communicating with the host. The attacker is able to intercept packets, then read and modify without anyone knowing of the attack, hence the term “man in the middle”. Granted, there are many other ways to implement a man in the middle attack, but this is just one example to show how easy it can be to implement.

2.3 Personal Laptops Turned into APs

An AP is a single-purpose device. It has no other use than to be an AP. Computers, PDAs, etc., are multi-purpose devices and could be used as APs. An AP sends beacons advertising itself. A wireless client talks to the physical layer, then listens for the AP beacon frames and remains in listening mode, waiting for a possible connection. Once a connection is established, you have two-way communications. This communication decides if you are a client, an ad hoc network, or an AP, based on the beacon frames. If there is no AP within range it keeps listening for a wireless network to connect to. With the appropriate software, a personal laptop can become an AP. This becomes a security nightmare because the laptop can now go from building to building, allowing anyone within range to connect to this “AP”.

Apple’s Airport automatically provides the ability to use its software to change from a client to an AP. When you go to the Network System Preferences in OS X, you can choose to “Allow this computer to create networks” when configuring Airport. This will cause your Apple laptop to advertise itself as an AP now, instead of as a wireless client. Unfortunately, by default, this is turned on and most users are unaware of the consequences of not turning the option off.

You can do this configuration from a PC laptop, as well, but it is not built into the operating system. Instead, you must find software that will let you configure the laptop to create networks and advertise as an AP. The thing to keep in mind here is that this whole issue is produced by a function of the software, not the hardware.

2.4 A Neighbor’s Legitimate AP

Two of the largest predicaments with a neighbor’s legitimate AP are: 1) the AP causes RF interference, and 2) the network is insecure. If the neighbor sets his AP in the same channel as yours, the strong signal you were previously getting can drop off dramatically. Although interference can be annoying, the bigger of the two problems is the fact that everyone within range can now see the neighbor’s AP.

There are security issues with associating with a neighbor's AP instead of your own campus network. When a neighbor's AP overlaps on your network, people will join the wrong network by mistake. If someone mistakenly connects to the wrong network, anything he does on his computer becomes available on the network. Not only is there an issue with unknowingly connecting to the wrong network, there are also people who will connect through this legitimate AP for the purpose of conducting illegal activities. The AP has its own traceable IP address; therefore the owner of the AP will be the one authorities come to if such activities take place.

2.5 Ad Hoc Networks

An ad hoc, or peer-to-peer, network allows the network interface card (NIC) to do the work of an access point by allowing users to switch the wireless NIC to ad hoc mode, thereby creating a wireless LAN. The NIC operates in independent basic service set (IBSS), which does not require an AP. Any computer in ad hoc mode can connect with other computers in ad hoc mode, just as if there were an additional WLAN.

If the NIC is set to infrastructure mode, only the AP sends beacons advertising itself. If the NIC is in ad hoc mode, the first machine establishes an IBSS and starts sending beacons. Other ad hoc machines then receive the beacon and accept, joining the ad hoc network.

While students may find this to be a great tool for sharing files without being on a network, there are several drawbacks. If users connect to an ad hoc network, they are only connecting to one another's computers. There would be no connecting to the Internet, servers, email, etc. Also, performance can suffer if there are several users connecting to the ad hoc network. When a Macintosh computer sees an ad hoc network once, the computer keeps looking for that network.

As for students using computers in class, professors should see to it that students do not have their NICs set to ad hoc mode. There have been many instances where students taking exams have their NICs set to ad hoc mode, thus sharing files and test answers.

3.0 Preventing Rogue Wireless Devices

Once you have defined the potential rogue wireless devices that may gain access to your WLAN, it is time to come up with a plan for preventing such devices on your network. Some of the methods of preventing rogue devices include creating security policies for your network; implementing an Acceptable Use Policy (AUP) for your users; using registration and authentication; Media Access Control (MAC) filtering and protocol filtering; performing regular security

audits; and educating users.

3.1 Creating Security Policies

When building a WLAN, it is critical to create and clearly define strong security policies, even before the first piece of wireless hardware is purchased. The network administrator should make policies that will protect the system's resources from unauthorized access. "System" in this sense applies to the network and every machine on campus that connects to it, along with the data on those machines.

The network administrator must first identify who will be on the deployment team. He should clearly define the roles of those team members. The administrator should determine who would be allowed to install APs and other wireless hardware. He should also determine who would have access to confidential information, such as encryption keys and AP passwords.

The physical security of APs must be taken into consideration. When the APs are deployed across campus, they must be mounted out of reach or view. Mounting behind ceiling tiles or in locked areas, where only authorized people have access, can meet this requirement. This is important to achieve in order to keep people from resetting the APs, which causes the network across the entire campus to become vulnerable. It also prevents hackers from being able to replace a legitimate AP with a rogue AP, as well as being able to steal an AP. However, the MAC addresses and locations of the APs should be listed so the WLAN team can easily find them.

The APs default passwords should be changed, as well. Strong passwords should be created by the WLAN administrator and should be given to only those authorized to have the passwords. The passwords should be changed regularly, particularly when there are changes in WLAN team members. Remember that if the passwords are not strong or changed when necessary, then unauthorized access to the APs could allow for configuration changes.

3.2 Implementing an Acceptable Use Policy

Once security policies have been set for the network, it becomes necessary to set policies for users. All universities and colleges set personnel policies and procedures for employees to follow. Those policies and procedures provide basic rules for attendance, leave, compensation, behavior, etc. The rules protect the employee, as well as the university. In a world of growing technologies, it is equally vital to set policies to protect the campus network. This policy is sometimes referred to as the AUP.

The AUP should clearly define what users can and cannot do while connected to the network. Some of the rules in the AUP are very basic, but go a long way

in protecting the network and its resources. For instance, the AUP should require that a university-supplied or -approved antivirus program must be installed on any computer connecting to the university-owned network. This prevents virus/worm threats from infecting the whole campus.

Other basic policies that should be included in the AUP are that users be required to maintain the most current OS patch level, use an approved personal firewall, use SNMPv3 or SSH for a secure connection to APs, and use a VPN client to provide proper levels of encryption and access control. These may not be WLAN-specific, but they warrant mentioning because they all have a part in protecting the network.

The AUP should include the university's policy on private APs, as well. Most universities have a strong stance on private APs. Some will allow the use of private APs in residence areas, as long as the APs do not cause interference with their own. On the other hand, many universities do not allow any private APs to be used in any university-owned building, including dorms. The schools have the right to prohibit the APs because they own the buildings and the network being used in those buildings. However, it is very important to include that policy in the AUP, as well as the procedures for dealing with non-compliance of the policy. The AUP must be reviewed and blessed by the General Counsel's office at each school. The General Counsel's office can make sure the policies you are creating fall within the limits of the law.

3.3 Using Registration and Authentication

Universities can have any number of ways to have people register their NICs before they can connect to the network. One such way is to use a registration server that allows you to authenticate with information in the Lightweight Directory Access Protocol (LDAP) directory. Every new student or employee is assigned a network identification (netid) and password when entered into LDAP. This netid and password becomes the key to gaining access to various servers and services across campus. When a new wireless computer or device needs to have access to the university's network, the student (employee) turns the computer or device on, goes to the browser, and is then taken straight to the registration page on the private network where he uses his netid and password to authenticate. Through the DHCP registration, the utility collects information and stores the MAC address. The registration utility then assigns an IP address that will then allow the user to use the network.

Some registration systems allow you to manually enter your MAC address. Unfortunately, this may allow for MAC cloning. However, if the registration utility has the ability to automatically collect and store the MAC address, the utility will be storing the MAC address for the machine or device that is connected at that time. Should an outsider try to connect to the school's network, he will continuously be taken to the registration page on the private network. Without

proper authentication on this page, the user will not get access beyond the small section of the private network. This is true for the wired or wireless network.

In the April 01, 2004, edition of Network Computing, Philippe Hanset, senior network engineer at the University of Tennessee, relates that users at UT are using this type of registration system. He says that once the users register, they can access the WLAN from anywhere at anytime. While this works, he admits that registration won't be as easy once the school makes the change to the new 802.11i wireless authentication and encryption standard. Once the change is made, the user will have to reauthenticate every time he opens his laptop. The alternative is to automate the authentication, but you lose part of the security in the process.[3]

3.4 MAC Filtering and Protocol Filtering

MAC filtering can become a university's first line of defense for its WLAN. Many schools have given up on using Wired Equivalent Privacy (WEP) as the only level of security because it has proven to be quite weak. The use of WEP was designed to be optional and it used only a single key for all users. Schools now use MAC filtering to monitor MAC addresses using the network. MAC filtering involves configuring the AP with a list of which MAC addresses are allowed to have access to the WLAN. When a client tries to join the WLAN, the AP compares the MAC of the requesting client with list of acceptable MAC addresses. If the client's MAC is on the list, it is able to authenticate. If the client's MAC is not on the list, it is denied access. Using MAC filtering, along with WEP, 802.1x, and/or other security measures, can deter hackers because it will consume more time the hacker isn't usually willing to waste.

An additional level of security would be to add protocol filters, as well. A protocol filter will allow, or not allow, specific protocols through the AP. By blocking large Internet Control Message Protocol (ICMP) packets, you have already taken steps toward preventing Denial of Service (DoS) attacks. You can also prevent changes to configurations by blocking users from accessing Simple Network Management Protocol (SNMP).[4] Keep in mind that defense-in-depth is the best security measure for any network.

3.5 Performing Security Audits

Security audits are important tools that should be done regularly as a preventative measure. Universities have administrative offices that handle auditing and so the auditing group should be responsible for conducting these audits. The preventative audit should cover the following:

- Physical security regarding the site for the APs – Is unauthorized access available?

- Security policies – Are the policies up-to-date? Are the policies enforceable?
- Configuration accuracy – Is each and every AP configured correctly?
- Power outages – What happens if there is a power outage or surge?
- Employee turnover – What changes need to take place to protect the WLAN?
- Neighboring networks – Are there other networks within range? Will these networks cause interference?
- Plan for intrusion detection – What happens when a rogue device is found?
- Plan for remediation – How do you get the network secure again?

While this is not an all-inclusive list for a preventative audit, it is a general start and additions should be made based on an individual campus's circumstances. For a good template on what to include in a security audit, there is a fairly comprehensive template in Wi-Foo: The Secrets of Wireless Hacking.[5]

3.6 Educating Users

One of the most underrated, yet one of the most important security measures is educating the user. Most users won't fully understand, or possibly care about, the technical details of securing the WLAN. However, teaching them the basics goes a long way, especially in a university, where education is a business!

When a new student or employee goes through his respective orientation, make sure he is given a copy of the AUP. Also, give him some materials about protecting (securing) his machine and the university's network and resources. The materials do not have to be lengthy, but should be informative and interesting enough to keep the reader's attention. Make the user feel that he is a critical part in keeping the network safe and working properly for those for whom it is intended.

Some of the most important things to educate users about (and why) include:

1. Strong passwords are needed for authentication.
   - A hacker can use utilities to break a password in a matter of seconds, allowing the hacker to have access to the user's and network's resources.
   - A stolen password can be used to gain access to resources and the user, not the hacker, would be the person being questioned.
   - A strong password that cannot be easily broken will quickly be bypassed by a hacker, thus protecting the user and the network from unauthorized access.
2. Ad hoc networks should not be used.
   - Using the ad hoc option opens a computer for anyone within range

to look at files on the user's computer.
- Using the ad hoc option may cause the user to mistakenly connect with the wrong network.

3. No private APs are allowed in university-owned buildings.
   - Unidentified, or unauthorized, APs cause interference with infrastructure APs.
   - The IT group cannot support unauthorized APs.
4. Do not click "Accept" for every digital certificate that appears.
   - The digital certificate may be a fake and by choosing to accept it could open up the network to attacks.
   - Know the basic information for digital certificates and verify the information before accepting the certificate.

It is proven that a policy is much easier to implement if the user understands why the policy must exist. The user will not feel as if the IT people are dictating rules for no reason and he will be more open to the rules.

4.0 Detection

If you have done a thorough job with preventing rogue wireless devices, then you should have nothing to detect. However, if a rogue device infiltrates your WLAN, your preventative measures should help you detect the device(s) quickly. There are basically two approaches used for detection: over wire or over air (RF).

4.1 Detection Over Wire

It is not possible to detect ad hoc networks over a wired network. However, it is possible to detect most other rogue devices over wire. Detecting rogue wireless devices over a wired network involves the use of some open source tools. One such tool is Nmap Security Scanner. Nmap (Network Mapper) is a free port scanning tool that is used on large networks or single hosts. It comes with a feature, TCP/IP fingerprinting, which can detect wireless APs across a wired network. Nmap has a database of TCP/IP fingerprints, which detects hundreds of operating systems, and includes wireless access points. Once the AP has been detected, the IP address assigned to that AP can be tracked down. Nmap is one of the most popular open source tools available and can be downloaded at http://www.insecure.org/nmap/. Nmap is available for most OS platforms.

An additional open source tool is Nessus, a vulnerability scanner. Using Nessus, the WLAN administrator can identify web pages, login banners, and other characteristics that help identify possible rogue devices. Also, Nessus has a plugin that specifically detects APs.

Another method of detection over the wired network is to compare MAC addresses in the Address Resolution Protocol (ARP) table with the MAC

addresses in the database for the AP. The Institute of Electrical and Electronics Engineers (IEEE) assigns the OUI (first 24 bits of the MAC address) to manufacturers, so each NIC can be uniquely identifiable. By using the OUI you can compare the first three octets of the MAC address to verify if it belongs to a wireless NIC or if it belongs to another device, such as a NAT box, router, AP, etc. This is not always a guarantee of accurate information, as some APs allow a user to do MAC cloning, which means the AP allows you to enter the MAC address of your wireless card instead of the AP.

4.2 Detection Over Air (RF)

It is easier to detect rogue wireless devices over air because of the very nature of wireless. On the other hand, it is more demanding to detect rogue devices over RF because it requires on-site detection versus the remote detection for the wire side. Since APs are constantly sending beacon frames advertising themselves, it is easy for the WLAN team to use various methods for detection.

Active probes are very valuable in detecting rogue wireless devices. An active probe sends a request out and waits to see if the beacon comes back, which verifies wireless activity is taking place. NetStumbler is a very popular open source utility that can be used on a Windows 2000 or XP machine with a wireless card. NetStumbler is available for download from http://www.stumbler.net. It is free, however donations are requested. MiniStumbler works just like NetStumbler, but is made for Windows CE devices. MacStumbler works the same, as well, except it is for Mac OS X. These utilities are used for war driving. With war driving, you can detect other networks that may be causing interference on your own network, but you can also detect rogue wireless devices. When doing war driving, use an omni-directional antenna to detect if rogue devices exist. However, to determine the exact location of the rogue devices, use a directional antenna.

NetStumbler is a valuable tool, as Demetrios Lazarikos reported in the November 10, 2004, edition of ComputerWorld magazine. Lazarikos spent the summer of 2004 driving through several large cities that prided themselves on the emphasis some of their higher-education facilities placed on IT security. In each city, Lazarikos spent very little time uncovering MAC addresses, SSIDs, and inventory lists for wireless networks in the area.[6] If one person can find so much information in a random pattern, imagine how NetStumbler can be focused on a university's campus, where there should be only one network in most cases, to detect unauthorized devices.

Passive probes listen to RF to see if there are APs or ad hoc networks. The utilities used for passive probes collect packets and recover encryption keys. These probes may force the AP to give out the SSID, since APs will eventually give the information you are looking for if you just keep asking. Kismet is one of the more popular passive probes. Kismet can be run on Unix/Linux machines,

as well as Windows machines running Cygwin. You can get Kismet at http://www.kismetwireless.net/download.shtml, along with a lot of Kismet patches and resources. Wellenreiter is another good Linux utility for network discovery and audits, and can be downloaded at http://www.wellenreiter.net/download.html. Here you will also find a version to be used with certain handheld devices, such as Ipaq.

Besides the software detection utilities, there are many enterprise-class intrusion detection systems (IDSes) available. For instance, Newbury Networks offers a package called WiFi Watchdog. This is a layered application that works with Newbury Networks' Locale Server and adds intrusion detection and includes live monitoring of users and devices, rogue AP detection, and even reports to WLAN administrators where the problems are.[7] Another well-known enterprise-class IDS is AirDefense Enterprise. AirDefense uses a server appliance and sensors to detect rogue devices. It tracks all rogue communication and provides forensic information about that communication.[8]

Remember that quantitative probes tell you if you have APs, while qualitative probes tell you if you have APs in a specific area. If you use multiple probes, they will intersect, with a higher probability of finding any and all rogue devices.

5.0 Remediation

Once you find rogue wireless devices, what comes next? The main goal is to secure the WLAN as quickly as possible. The first step is to shut down the port if detected on the wired network, then find the culprit and deal with him. Have your university's audit group do another security audit. Finally, you may have to seek solutions with an enterprise-class source.

5.1 Disable the Port

If the rogue device is found through detection on the wired network, have the wired networking group disable the port. This does not fix the RF problem, but it certainly works on the traffic.

5.2 Find the Culprit

Once you track down the rogue device, find the owner and confiscate the device. This is when the AUP will come in very handily. If your school's AUP covers this area fully, then follow through with what the AUP says will happen. The school's legal counsel has approved this document, so the WLAN administrator should be fully backed when carrying out the consequences as determined by the AUP. If it is obvious that the rogue device was not intentionally deployed (i.e., a user did not turn off the option to "Allow this computer to create networks") this may be the perfect time to do some one-on-

one user education.

5.3 Do Another Security Audit

If your prevention tactics have not been successful in preventing rogue devices, it would be good to have your university's audit group do another security audit. The audit can show where the breakdown(s) occurred. The WLAN administrator can then make the appropriate changes for tightening the network. Make sure the audit is fully documented and retained for future reference.

5.4 Seek Solutions From an Enterprise-Class Source

If your WLAN seems to have repeated problems with rogue devices infiltrating the network, it may be necessary to use enterprise-class solutions. AirDefense, again, offers a great solution that not only prevents and detects rogue devices, it also mitigates the risk automatically or through a set of pre-defined policies. AirDefense Enterprise is customizable, manages itself, and terminates the rogue devices for you.[9] AirDefense sends a message to the AP, using the 802.11 protocol to shut off. An exclusion network is built to keep from shutting down specific networks.

Aruba Networks and Sygate have partnered to offer a customized integrated enterprise-class solution using Sygate Secure Enterprise, Sygate's endpoint security solution, along with Aruba's new grid controller system. Bob Johnson, director of Network Services at Dartmouth College said in a press release announcing the product that the product allows users to be in a trusted state and comply with Dartmouth security policies no matter where they are connecting to the network.[10] If users on a network with this solution are not compliant, they will be denied access, quarantined, or directed to a remediation server.

6.0 Summary

When securing your university's wireless network it is of the utmost importance to define the potential rogue wireless devices that may infiltrate your WLAN. You must know what you are looking for before you can protect against it. After defining what you consider rogue wireless devices to be, you must take a proactive stance in the prevention of rogue devices. If you have not been able to fully prevent rogue devices on your WLAN, you must be able to detect them at once. Finally, if and when a rogue wireless device is detected, you must be reactive in immediately remedying the problem so your network will be secure once again.

References

[1]Batheja, Aman. "WiFi dispute gets UTD students in uproar." Fort Worth Star Telegram. 22 Sept 2004. 10 Jan 2005. http://www.utwatch.org/oldnews/fwst_wifi_9_22_04.html.

[2]American Radio Relay League. "FCC Queries Wireless Internet Provider About Interference to Hams." 15 Feb 2001. 12 Jan 2005. http://www2.arrl.org/news/stories/2001/02/15/2/?nc=1.

[3]Higgins, Kelly. "University of Tennessee Implements 802.1x No WLAN User Left Behind." Network Computing. 01 Apr 2004. 01 Feb 2005. http://www.nwc.com/showArticle.jhtml?articleID=18401548.

[4]Barnes, Christian, et al. Hack Proofing Your Wireless Network. Massachusetts: Syngress Publishing, Inc., 2002.

[5]Vladimirov, Andrew A., Konstantin V. Gavrilenko, Andrei A. Mikhailovsky. Wi-Foo: The Secrets of Wireless Hacking. Boston: Addison-Wesley, 2004.

[6]Lazarikos, Demetrios. "My Summer of War Driving." ComputerWorld. 10 Nov 2004. 31 Jan 2005. http://www.computerworld.com/securitytopics/security/story/0,10801,97352,00.html.

[7]Griffith, Eric. "Pinpointing Problems with Live Monitoring." Wi-Fi Planet News. 04 Dec 2002. 31 Jan 2005. http://www.wi-fiplanet.com/news/article.php/1551731.

[8]AirDefense Enterprise Wireless Security Features Web Page. 01 Feb 2005. http://www.airdefense.net/products/features/security.html.

[9]AirDefense Enterprise Home Page. 01 Feb 2004. http://www.airdefense.net/products/enterprise.html.

[10]Sygate. "Sygate Teams with Aruba to Eliminate Rogue Devices from Wi-Fi Networks." Sygate Press Release. 15 Nov 2004. 01 Feb 2004. http://www.sygate.com/news/sygate-aruba-wireless-endpoint-security.htm.