Overview of Security Threats & Maintaining & Monitoring the Security WLANs

By Sandeep Natekar

With the proliferation of WLANs in every home/office environment and their use in carrying out important business transactions, maintaining and enhancing the security of WLANs has become very important. Moreover, with Federal Regulations in place to enforce security of business transactions using WLANs, deploying a secure, 'crack-proof' WLAN has become a complex task. This also requires the monitoring of WLANs to check for adherence to Federal policies and detect and identify the policy violators.

The 802.11 standard had stipulated Wired Equivalent Privacy (WEP) as the principal encryption scheme. It wasn't too long before it was found that WEP encryption was a hacker's delight and that the encryption could be easily cracked using rudimentary hacking tools. IEEE task force 802.11i was formed to look into the weaknesses of WEP and develop enhancements to the security layer of 802.11'b'. While the 802.11'i' task group was taking way too long to finalize its work, the WiFi Alliance (a group of companies manufacturing WiFi equipment) agreed upon the use of the WPA (WiFi Protected Access) security, which is an enhancement to WEP, but much more robust than WEP. The IEEE 802.11i task group finalized on 802.1X for authentication (entailing the use of EAP and an authentication server), RSN (Robust Secure Network) for keeping track of associations, and AES (Advanced Encryption Standard) -based CCMP (Cipher Block Chaining Message Authentication Code Protocol) to provide confidentiality, integrity and origin authentication. These will be looked at in detail.

Having secured your WLAN with the appropriate mechanisms in place, the next step would be to monitor the network. One might question the need for elaborate monitoring tools in spite of seemingly invincible security mechanisms already employed to fend off intruders and hackers. However, the most surprising fact about any WLAN is that most of the time, the WLAN is made insecure and vulnerable to external threat by authorized users of the WLAN themselves. Unwary actions such as improper system settings or installation of additional insecure access points can open up the whole WLAN to an external threat. Moreoever, recent federal policies such as SOX, HIPAA, GLBA, etc. have made it mandatory to monitor WLANs 24x7 in places like hospitals, banks and large corporations where important data is handled. This puts monitoring of WLANs on par with securing them.

Any discussion on WLAN security has to be made in the context of the "casual eavesdropper" and an "intentional hacker."

CASUAL EAVESDROPPER VS. MALICIOUS HACKER

Any discussion on WLAN security has to be made in the context of the "casual eavesdropper" and an "intentional hacker." WLAN security discussion in the context of casual eavesdropper is different from that made in the context of an intentional hacker. An intentional hacker is one who is intent upon breaking into your WLAN no matter what and will use sophisticated tools. He is also far more patient in achieving his mission and is willing to spend a lot of effort in achieving his end. His goal is to break into your WLAN for the sake of sabotage or financial gains. A casual eavesdropper on the other hand is one who has no serious intentions of breaking into your WLAN for the purpose of financial gains or sabotage. He is, for the most part, a "cheapskate" who wants to latch onto your WLAN to access the internet without paying for it. He wouldn't use any sophisticated technology for this purpose but will rely on by chance associations with your WLAN access points.

HOME VS. OFFICE ENVIRONMENTS

Let us begin our analysis of security threat to a WLAN starting from the home environment. Most of us who use laptop computers (and even some who use desktop) now have a wireless router connected to our cable/DSL modems in our homes. The convenience of Wireless Networking within our homes coupled with the affordable prices of wireless access points, routers and adapters has tempted most of us to set up home wireless networks. In home environments, we face the problem of casual eavesdroppers who very readily connect to our home network and use the Internet service we pay for. In domestic environments, such "cheap associations" are generally for the purpose of casual web-browsing, email or downloading/streaming videos and music. However, it is always we who have to suffer the overindulgence of such casual evesdroppers at our expense. The problem is particularly compounded for people who live in apartments. When I first installed a Wireless network at home, I was shocked to discover the number of network associations my Access Point was handling, all unauthorized except mine. However, assuming that most of us have benevolent neighbors, such unauthorized associations in domestic environments

are fairly docile, and do not pose a very serious threat.

WEP FOR HOME, WPA FOR THE OFFICE

The IEEE 802.11 standard does specify WEP (Wired Equivalent Privacy) as the Encryption Algorithm to be followed, but it is well known for its inherent weaknesses. WEP is known to be cracked using well-known tools such as Netstumbler and other freely downloadable software from websites. WEP may be a good WLAN security solution at home, since a casual eavesdropper would only connect to your network for the purpose of saving a few bucks. WEP does solve the problem of exposing your home network to casual eavesdroppers and can isolate your WLAN for your exclusive usage.

Now if we move our focus to a large office complex housing offices, an unauthorized user having malicious intent can hack into the company's network and cause irreparable harm.

It is in such a situation that a robust security mechanism for the WLAN becomes imperative and worth implementing. WEP may be too flimsy a security encryption in this case (WEP has been cracked in as few as 3 minutes). Following the failure of WEP, IEEE came up with 802.11 "i" as an enhancement to 802.11 security. Meanwhile, companies which form the WiFi Alliance came out with their security mechanism called WPA (WiFi protected Access) in their products as a solution to WEP failure. WPA provides stronger encryption when compared to WEP as it uses dynamic keys for encryption. This means that every data packet is encrypted using a unique key. WEP uses the same key for all the data packets during transmission. WPA also specifies a new authentication mechanism, in which the authentication operation is transferred from the Access Point to an authenticating server. The server will then authenticate the client and the client can then associate with that AP.

However, the greatest drawback of WPA is its vulnerability to Denial-of Service (DoS) Attacks. If a user is trying to get in and sends two packets of unauthorized data within one second, WPA will assume it is under attack and shut down.

While this feature is designed to safeguard against breaches of security, it presents a prime opportunity for a hacker. The only thing they need to do in this situation is send data frames periodically, causing constant shutdowns. The

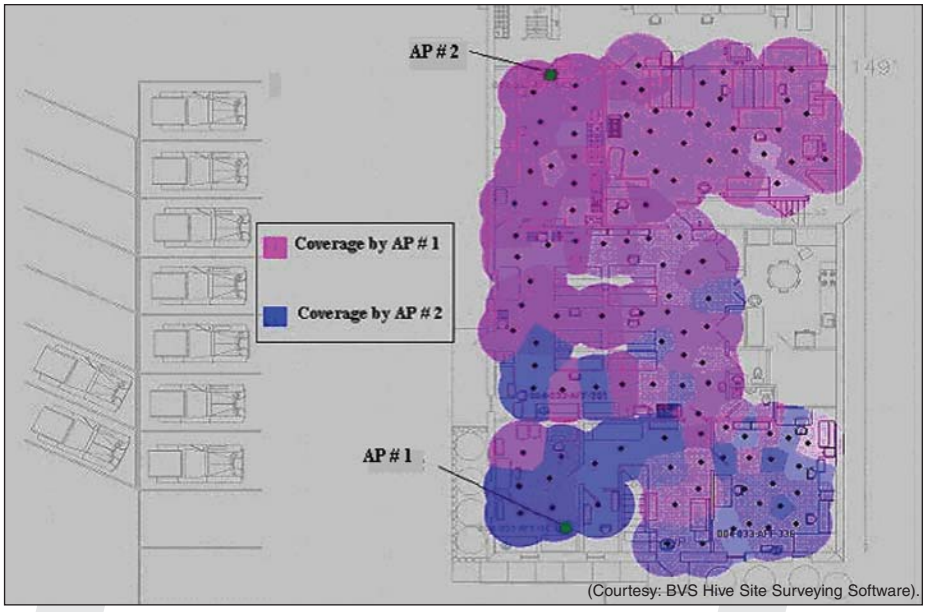

Figure 1: Coverage of AP's using site surveying software

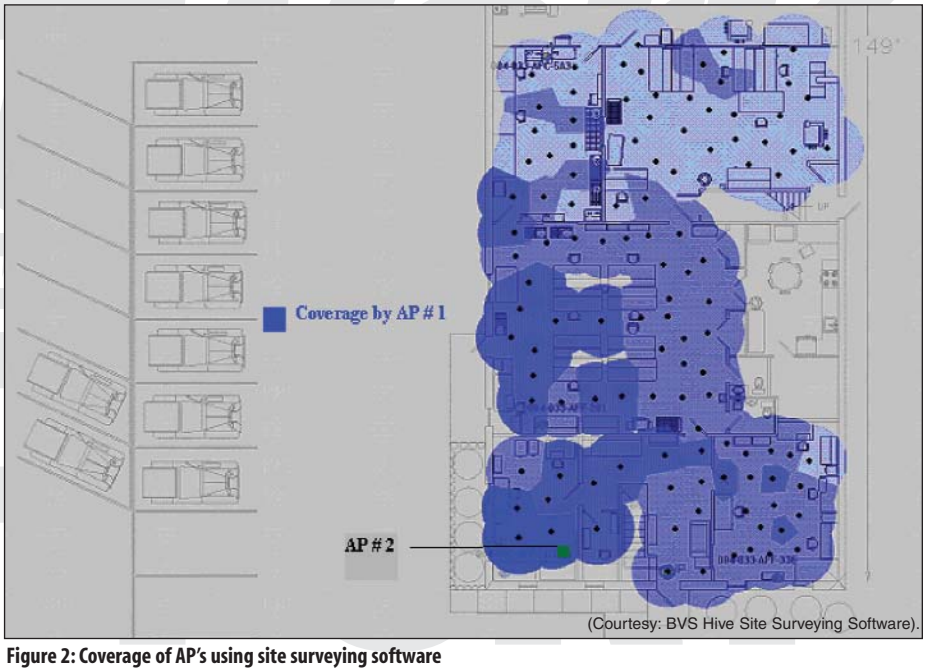

Figure 2: Coverage of AP's using site surveying software

hacker may be difficult or impossible to find because they don't need to use much transmit power or utilization of the network.

The most fundamental ways by which you can shield your WLAN against DoS attacks is by having the most up-to date Firewall systems in place. Use of strong and difficult-to-unearth passwords can also help in minimizing the possibility of such attacks. However, the best possible defense against such attacks, and also the most difficult and expensive method, is to insulate your building against external RF penetration. This could be done by grounding your interior walls, using metallic tint on windows instead of blinds and also coating walls with metallic paint. Perform site-survey tests to minimize RF leakage outside your premises.

It is important to note there is no such thing as 100% security implementation. Moreover, in the case of WLANs, the only way to achieve near 100% security is not a practical feasibility. However, even if a WLAN is not secure, implementing strong security mechanisms can no doubt deter a potential intruder or hamper his morale in hacking into your network.

While the threat from intruders is no doubt a serious threat, it is shocking to note that most of the time, it is the internal, authorized members of the WLAN that make it most vulnerable to external threat. Unhealthy practices by

employees can open up a completely secure network and make it a hacker's delight. Apart from implementing the best available security mechanisms, following certain simple steps can help in increasing the security level of your WLAN:

- Disabling SSID broadcasts can reduce the chances that your network can be visible to the casual eavesdropper. Although this has been touted as a no-use practice by a lot of people, it is infinitely better than letting the world know of the presence of your AP, many times a second.
- Using Open system authentication instead of Shared Key authentication and configuring your wireless router accordingly. Shared Key authentication makes a lot more information available to the hacker to hack into your account than Open System authentication.

INTERFERENCE: A MAJOR SECURITY CONCERN

Phew! We have now taken care of the casual eavesdropper as well as the intentional hacker and are now assured of a high degree of security and good performance from our WLAN. However, sometimes, we come across a stage when our WLAN may seem very slow or we may receive data in bursts. For example while using an IM, although the other person is sending us a lot of messages, we do not see it for a while, and then suddenly all his messages appear in a huge burst. This is sometimes quite frustrating when downloading large files or even while sending emails. This apparent sluggish performance and drop in throughput rates is caused by interference from other high power sources such as Microwave ovens, cordless phones, neighboring WLANs on the same channel or frequencies as ours, and other transmistters in the WiFi spectrum.

Interference from other 802.11 and 802.11 non-compliant sources is a major concern in WLAN security. WLAN interference sources such as Microwave ovens and 2.4GHz cordless phones should be studied for interference and their frequency/band of operation must be identified. It has been found that Bluetooth devices generally do not interfere with 802.11b WLANs, so that's a relief. Adjacent WLANs should be made to operate on non-overlapping channels such as 1, 6, and 11. Microwave ovens from different manufacturers are known to operate in different regions of the WLAN spectrum. Hence if you have a Microwave oven in your office, figure out what region of the spectrum it operates in. The AP should then be set on a channel which does

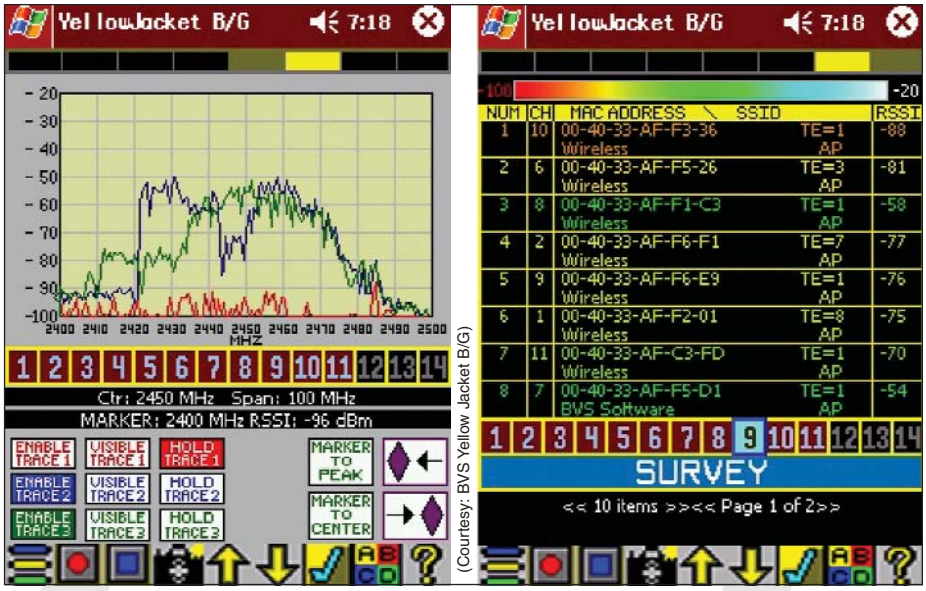

Figure 3:Pocket PC based handheld WLAN monitoring application

BVS BEEKEEPER CHANNEL SURVEYOR 08/30/05 16:18:01

#	MAC ADDRESS	STA	CH	[SSID/BSSID]/Mode/WEP	dBm	SNR	FIRST	LAST	AUTH?
1	00-40-33-AF-F1-C3 ADDTRON TECHNOLOGIES.	AP	8	Wireless	-54	36	08/30/05 16:16:28	08/30/05 16:17:59	NO
2	00-40-33-AF-F2-9D ADDTRON TECHNOLOGIES.	AP	4	Wireless	-21	69	08/30/05 16:16:28	08/30/05 16:18:01	NO
3	00-40-33-AF-F6-F1 ADDTRON TECHNOLOGIES.	AP	2	Wireless	-30	60	08/30/05 16:16:28	08/30/05 16:18:01	NO
4	00-40-33-AF-C3-B6 ADDTRON TECHNOLOGIES.	AP	5	Wireless	-25	65	08/30/05 16:16:28	08/30/05 16:18:01	NO
5	00-40-33-AF-F3-36 ADDTRON TECHNOLOGIES.	AP	10	Wireless	-35	50	08/30/05 16:16:28	08/30/05 16:18:01	NO
6	00-E0-03-04-1C-2C NOKIA WIRELESS BUSINESS COMM.	NIC	11	instawave /ad-hoc	-21	69	08/30/05 16:16:30	08/30/05 16:18:00	YES
7	00-40-33-AF-C3-FD ADDTRON TECHNOLOGIES.	AP	11	Wireless	-28	62	08/30/05 16:16:31	08/30/05 16:18:01	YES
8	00-11-24-03-5B-D1 Apple Computer	AP	11	Apple Music Network	-79	11	08/30/05 16:16:34	08/30/05 16:17:52	YES
9	00-0C-41-DC-4E-F0 The Linksys Group, Inc.	AP	11	linksys/WEP	-90	0	08/30/05 16:16:39	08/30/05 16:17:51	NO
10	00-0F-34-46-BA-6C Cisco Systems	AP	1	copper	-90	0	08/30/05 16:16:54	08/30/05 16:17:56	NO
11	00-06-F4-04-BB-EF Prime E'tronics. & Satellitics.	NIC	11	00-11-24-03-5B-D1	-30	60	08/30/05 16:17:51	08/30/05 16:17:13	YES

Scanning Channel # 6 Unauthorized MAC Detection Alarm: OFF

Figure 4: Wireless device properties obtained during a scan.

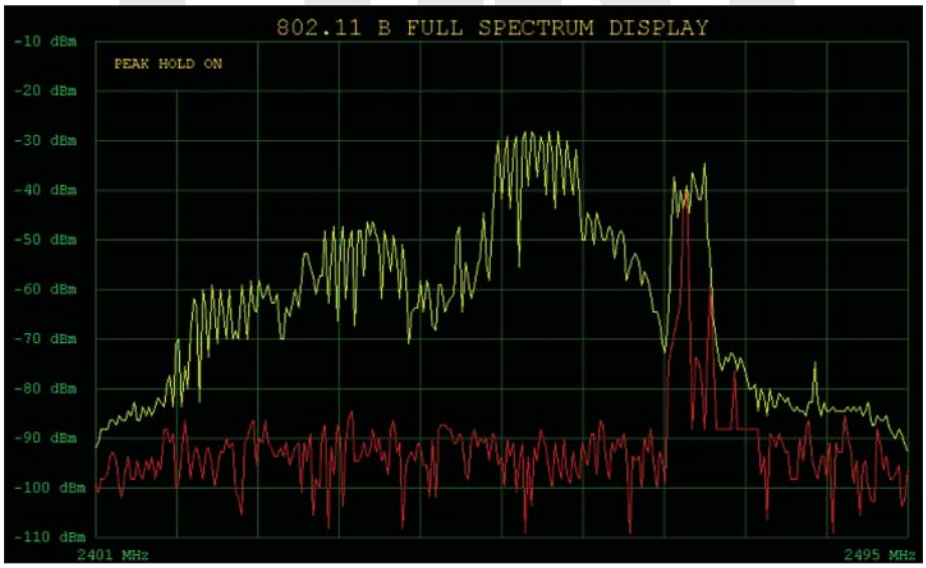

Figure 5: Microwave Oven in the 2.4GHz band

not overlap with your microwave. This might not always work, but it is always worth a try. Cordless phones which operate on 2.4GHz band are a major source of interference and hence their use must be avoided. It is wiser to switch to 900MHz cordless phones to completely eliminate interference from their use in the 2.4GHz band.

Before deploying WLANs, it is important to perform an RF site survey of the facility. RF site surveys can give a good idea of the number and locations of AP placements, signal coverage, regions of co-channel interference and signal leakage.

RF SITE SURVEYS

Before deploying WLANs, it is important to perform an RF site survey of the facility. RF site surveys can give a good idea of the number and locations of AP placements, signal coverage, regions of co-channel interference and signal leakage. This way, you can obtain a good picture of how good or bad your WLAN will be after deployment and can help in planning the deployment of our WLAN for optimum performance and minimum interference.

Figures 1 and 2 show the coverage of APs mapped using a site surveying software. Figure 1 shows the coverage of two APs as mapped by the software. It is interesting to observe how the RF energy from AP #2 penetrates into areas closer to AP #1 even though they may be separated by a distance of 100 feet and have solid walls between them. Figure 2 shows the coverage of AP #1 alone, in the absence of AP #2. Thus if AP #1 and AP #2 are on the same channel, there could be sufficient interference from AP #1 to cause a reduction in throughput rates of transmission by AP #1. This is also applicable to microwave ovens which are known to leak out RF energy (in some cases, of unbelievable and harmful power levels) in the 2.4GHz sufficient to cause a complete shutdown of your Wireless LAN.

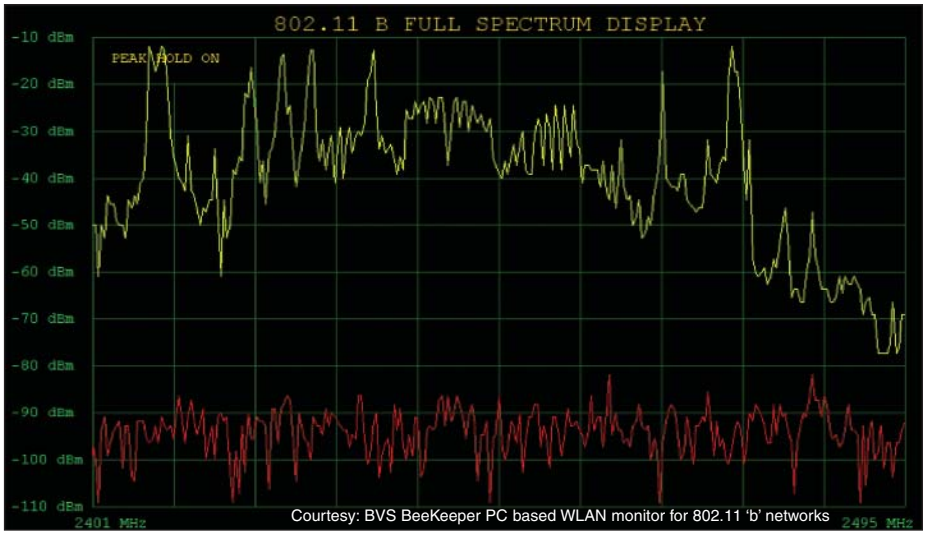

Figure 6: 802.11 Frequency Hopper

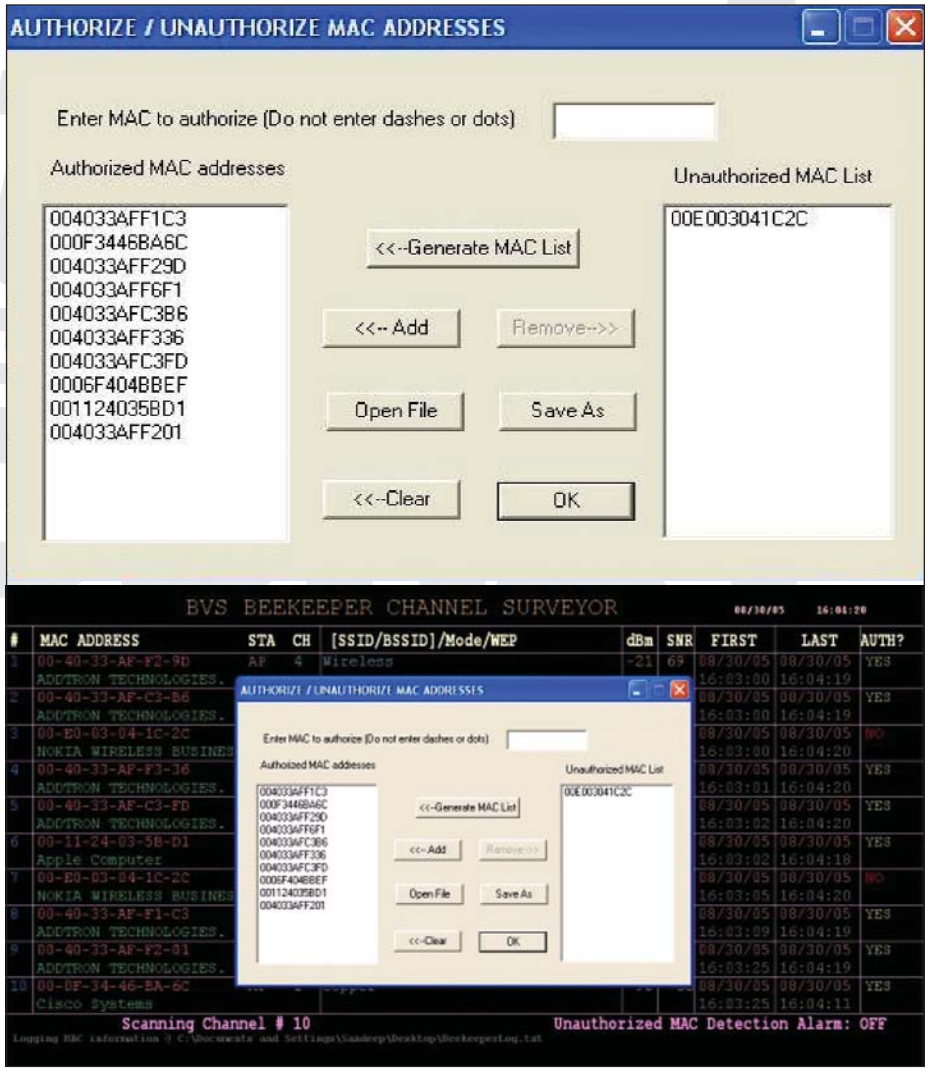

Figure 7: Setting up an Access Control List

WLAN MONITORING

After taking care of the security and interference issues, the next important step would be to install mechanisms to monitor WLAN security. Monitoring WLAN security is almost as important as having the right security nuts and bolts in the network. This is because WLAN security is made vulnerable to interference and threat from authorized users

within the WLAN. Improper practices can seriously disrupt the WLAN. More recently, WLAN security and integrity monitoring has gained newfound importance due to Federal policies mandating practices that prevent malpractices, fraud, and data theft.

Due to the increasing security and performance concerns, a WLAN has to be monitored for:

- Detecting intruders.
- Supervising if authorized users within the WLAN are configured to conform to the health of the WLAN.
- Detecting the presence of prohibited devices within a WLAN and identifying them.
- Identifying sources of interference and their location within the spectrum.
- Logging Information for recording and reference.

WLAN monitoring applications are a hardware-software package. The hardware is typically a sensor(s) which can be a receiver or a tranceiver in the form of a Network Interface Card (NIC). A WLAN monitoring sensor is generally a packet capture device which captures packets passively. A good sensor must be able to scan all (or a desired pre-configured number) the channels continuously at the rate of a certain number of seconds per channel. It must also have the capability to be parked on one of the channels for additional scruitiny. The receiver must have the capability to provide Packet Error Rate information, Multipath propagation analysis. Moreover, the receiver should not only capture beacon packets, but also data packets as a lot more information is available in the non-payload section of the data packet.

The software could be a PC application or a Pocket PC Windows CE application. Applications which run on a Pocket PC make portable WLAN monitoring easy and simple. If WLANs in very large facilities or tall buildings are to be monitored, the multisensor WLAN monitoring packages can be extremely helpful. For monitoring WLANs located in different parts of the country or even the world, or one central location across the internet, IP enabled WLAN monitoring applications can be a big help.

A good WLAN software application will use the captured packets to display the list of detected MAC addresses, their SSIDs, the name of the Vendor who manufactured that device, the measured signal strength and signal-to-noise ratio (SNR). Additional useful features would be to display when the device was first detected and when it was last seen. Bonus features on it would be displaying the Encryption type and identify the device to be an Access Point (AP) or a Network Interface Card (NIC). Better still would be its capacity to identify if a certain NIC is associated with an AP or is in an ad-hoc mode of operation. Ideally, a good WLAN monitor will monitor the RF passively, without making its presence known by actively transmitting.

BVS BEEKEEPER CHANNEL SURVEYOR 08/30/05 16:18:01

#	MAC ADDRESS	STA	CH	[SSID/BSSID]/Mode/WEP	dBm	SNR	FIRST	LAST	AUTH?
1	00-40-33-AF-F1-C3 ADDTRON TECHNOLOGIES.	AP	8	Wireless	-54	36	08/30/05 16:16:28	08/30/05 16:17:59	NO
2	00-40-33-AF-F2-9D ADDTRON TECHNOLOGIES.	AP	4	Wireless	-21	69	08/30/05 16:16:28	08/30/05 16:18:01	NO
3	00-40-33-AF-F6-F1 ADDTRON TECHNOLOGIES.	AP	2	Wireless	-30	60	08/30/05 16:16:28	08/30/05 16:18:01	NO
4	00-40-33-AF-C3-B6 ADDTRON TECHNOLOGIES.	AP	5	Wireless	-25	65	08/30/05 16:16:28	08/30/05 16:18:01	NO
5	00-40-33-AF-F3-36 ADDTRON TECHNOLOGIES.	AP	10	Wireless	-35	50	08/30/05 16:16:28	08/30/05 16:18:01	NO
6	00-E0-03-04-1C-2C NOKIA WIRELESS BUSINESS COMM.	NIC	11	instawave /ad-hoc	-21	69	08/30/05 16:16:30	08/30/05 16:18:00	YES
7	00-40-33-AF-C3-FD ADDTRON TECHNOLOGIES.	AP	11	Wireless	-28	62	08/30/05 16:16:31	08/30/05 16:18:01	YES
8	00-11-24-03-5B-D1 Apple Computer	AP	11	Apple Music Network	-79	11	08/30/05 16:16:34	08/30/05 16:17:52	YES
9	00-0C-41-DC-4E-F0 The Linksys Group, Inc.	AP	11	linksys/WEP	-90	0	08/30/05 16:16:39	08/30/05 16:17:51	NO
10	00-0F-34-46-BA-6C Cisco Systems	AP	1	copper	-90	0	08/30/05 16:16:54	08/30/05 16:17:56	NO
11	00-06-F4-04-BB-EF Prime E'tronics. & Satellitics.	NIC	11	00-11-24-03-5B-D1	-30	60	08/30/05 16:17:51	08/30/05 16:17:13	YES

Scanning Channel # 6 Unauthorized MAC Detection Alarm: OFF

Figure 8a: Sample AP with MAC address

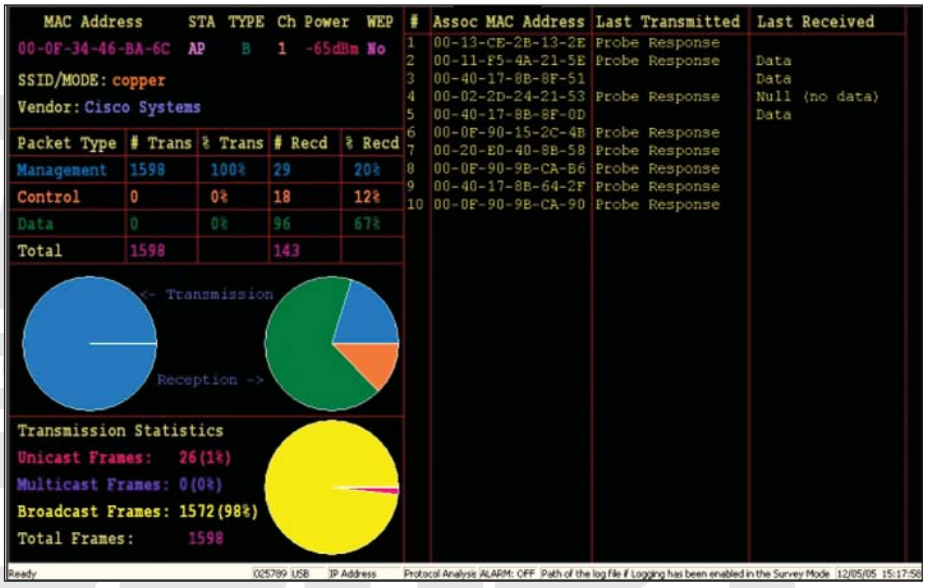

Figure 8b: Sample AP with MAC adress

INTERFERENCE MONITORING

Consider a scenario where you have a good WLAN monitor which gives you all the relevant information about a detected device. When you see that Device List, you see all authorized devices within your WLAN and each one seems to have permitted configuration. In spite of this, your network is sluggish and tends to go dead from time to time. If your WLAN monitor can detect interference or anomalies within the WLAN spectrum which may be the cause of your network disruptions. If your WLAN monitor can give an indication as to which region of WLAN spectrum the interference lies and what its signal strength is, it can help to find the source and shut it off.

Athough a WLAN may be well secured for keeping intruders at bay, there is always a chance that a determined hacker may be lurking nearby to gain access. Hence it is of paramount importance to even detect the presence of casual eavesdroppers and turn them away. A good WLAN monitor will let the WLAN administrator create an Access Control List (ACL). This ACL can comprise of the list of MAC addresses which are authorized within the WLAN. The monitor

must then flag any device which is not included within the ACL as 'Unauthorized' to detect its presence. Audible alarms can be set to go off every time an unauthorized device has been detected to alert the WLAN administrator.

DETECTION OF ASSOCIATED NETWORK INTERFACE CARDS

Typically, APs transmit at a higher power than NICs. Hence even for a good WLAN monitor, the chances that it will detect an AP located at a certain distance is much more than it will detect a NIC at the same distance. Thus, although a WLAN monitor will be able to detect this AP, it might not detect the NICs associated with this AP. These NICs could well be accessing information from the network to which this AP belongs and these could well go undetected. It is imperative to detect and identify devices associated with an AP so as to prevent covert access to your WLAN.

As an example, in Figure 8a although the AP with MAC address 00-0F-34-46-BA-6C and SSID "coppper" shows up in the Channel Survey mode, clients associated with it do not show up. This could be due to the fact that the signal from the clients may not be picked up by the receiver to process and display information about their presence.

In figure 8b, which shows the analysis of the same MAC address, it can be seen that there are ten clients who are communicating with the same device. If any of these clients are unauthorized, then it could result in a serious breach of WLAN access policies and a failure of the security enforcements.

DATA LOGGING

Data logging is another good feature in a WLAN monitor and a good practice for WLAN administrators to adopt. This will help to keep records of WLAN activity for corporate reports and references. This can also be helpful in studying WLAN activity behavior and traffic patterns at various times during the day. The DoD regulatory guidelines on the use of WLANs have made reporting WLAN usage mandatory. Even Federal regulations such as SOX, HIPAA, and the GLBA have made reporting of WLAN activity in areas of health care, banks, financial services, and large corporations compulsory. Consequently, data logging can also assist in future WLAN planning and deployment by using statistical prediction and analysis.

REMOTE CONNECTIVITY

A good WLAN monitor will allow the user to connect to the hardware sensor or receiver remotely so as to allow remote and centralized access. This will allow the user to be located anywhere in the world and monitor sites of his interest. Such a capability would be particularly useful for military and government WLAN administrators. For example, WLANs in all of the DoD facilities within the U.S. can be monitored in the Pentagon or some other such centralized location by placing the appropriate sensors in each of the remote locations. This will not only lead to better WLAN administration, but will also alert the central authorities in a timely manner upon detection of any unauthorized Wireless activity. Even for a large corporation, which has factories and establishments all over the world, all of the monitoring can take place centrally, provided the appropriate hardware is in place in the remote locations.

CONCLUSION

WLAN security is easy to achieve to deter the casual eavesdropper; the same task becomes daunting when it comes to the malicious hacker. Moreover, the more secure a WLAN, the more determined and intelligent would the intentional hacker be and he would possess the latest and most up-to-date technology to counteract the WLAN security mechanisms. However, even the most intelligent and well-equipped intruder can be kept at bay by educating authorized WLAN users to follow simple practices. Site surveys and RF planning can help efficient WLAN coverage and save a lot of resources. Interference detection, minimization or elimination will help improve overall WLAN performance. Last but not least, intelligent WLAN monitoring and administration prevents malpractices within the WLAN and supports the overall performance of the WLAN.