Global Information Assurance Certification Paper

Analysis of Wireless LAN Security

By Patricia Roberts

Abstract

When companies refer to mobility, often they refer to the ability of employees to work from home, hotel rooms or airports. However, with the introduction of wireless LANs, mobility is provided even within the office environment.

Wireless technology has arrived. It provides workers with the benefit of working faster and more efficiently in almost any location. When people see the advantage of a wireless network infrastructure and the flexibility it brings, it becomes increasingly difficult for companies not to do the same. There is the disadvantage, however, that it can pose immense danger to a corporate network if it is not implemented correctly. All it takes is for one PDA or laptop to find a rogue wireless network device and many confidential secrets can be disclosed within seconds. Many companies are keen to employ a Wireless LAN infrastructure, however, there is the worrying issue of security, which continues to prevent them from doing so. Companies have realised that wireless technology has arrived and it is less dangerous to embrace it than to ignore it.

This paper aims to identify the main security threats to WLAN infrastructures, to look at some products that are currently available on the market and also steps that should be taken to ensure a secure Wireless network within a corporate environment.

Security Threats

Wireless LANs are open to many security threats if they have not been implemented correctly. The possibility of breaking into a company's internal network by accessing them from the inside, bypassing external firewalls, is a very real threat. In a wired environment it is reasonable to assume that an external firewall will prevent hackers from gaining access to the internal network. For this reason, many of the business critical systems can be safely placed on the LAN behind a firewall. However, there are many cases in which employees install rogue access points directly onto the company's LAN. Most often these rogue access points are badly configured (if at all!) and provide hackers with a means of accessing that particular company's network and making any firewall checks and restrictions redundant. This can often lead to the crippling of business critical systems by malicious hackers.

Denial of service (DoS) attacks can make 802.11 networks unusable by jamming the available radio frequency (RF) spectrum. This type of attack adds overhead onto the available bandwidth taking it away from legitimate users, forcing the network to essentially shut down. There are also other radio devices that operate on the same frequency as 802.11b devices, such as Bluetooth and cordless phones. If there are too many of these devices in the same area as a WLAN, the performance will be greatly affected.[1]

Wireless LANs are open to attacks from internal sources as well as external. Internal attacks can come from rogue access points, insecure configurations on wireless LAN devices and accidental associations - to name but a few. Internal attacks will now be looked at in greater detail.

Rogue access points have already been discussed briefly, but what are they exactly? Rogue access points occur when employees install their own home networking access point without seeking management permission and without adhering to any security policies, which may be in place - but which most often times are not. It is often the case that an employee may have recently installed a wireless network at home, seen the benefits of having one and decided to introduce it in the office environment without realising the security risks of doing so. These devices pose a blind risk to network security managers. Rogue access points can also be difficult to detect as they can quickly and easily be unplugged from the network; for example, an offending employee may see that network administrators are walking around with handheld wireless devices sniffing for rogue access points, all he needs to do is to simply disconnect it or turn it off, thus tricking the managers into believing it is not there. Rogue access points may be employed quite innocently or mischievously, but whichever the case, they extend the corporate network beyond the confines of the corporate building, hence exposing the corporate network to attack by criminal hackers. It is imperative that there are no rogue wireless LAN access points on a corporate network. [2] [3]

Insecure configurations also pose a problem to the secure deployment of wireless LANs. Configuration settings including default or weak passwords, SSID broadcast, no authentication requirements and weak encryption can all lead to the access point becoming an open gateway for network intrusion. There is also the concern that even though management may deploy a properly configured access point, it may be possible that employees who want increased operability can reconfigure it. Many access points are reset to default configuration settings when there is a system failure or when a power interruption or surge occurs. Any reset would leave the access point and the network in a very vulnerable state.

Accidental association with another network can occur when a neighbouring company has employed a wireless LAN, which bleeds into another company's

physical location. This can often happen in the case of high-rise buildings where one company is located on the floor above another, with very little physical space separating them. There is currently a security issue with WindowsXP that can often lead to a situation of accidental association. WindowsXP has a default configuration to automatically associate with any broadcasting access point. This means it is constantly actively looking for a wireless network with which it can connect. This process of active searching can result in users associating with rogue access points or other badly configured wireless LAN devices and sometimes even without either party realising. When this situation occurs it is possible that the user may end up sending private, sensitive information onto a foreign network. The risk to a particular company, X, is that its users may associate with another network as well as external users associating with the Company X network. This can lead to various security issues including the disclosure of sensitive information such as usernames and passwords and may even lead to the bridging of two company networks.

Up to this point, this paper has discussed the internal threats to a wireless LAN; rogue access points, insecure configurations and accidental association. There are, however, external threats, which must also be considered. These include war driving and chalking, eavesdropping, man in the middle and sophisticated attacks.

War driving is a past time of hackers, which involves driving around a city looking for open wireless networks that they can connect to. Hackers often use war chalking to share their discoveries with other hackers. People who carry out war chalking claim that they simply want to get free internet access and wish to share the locations for doing so with their friends. Nonetheless, warchalking advertises the fact that a corporate network is open and provides a free starting point for malicious hackers. Warchalking involves using symbols sketched on walls or pavements detailing SSID information, available bandwidth and WEP code information. The definition of warchalking is

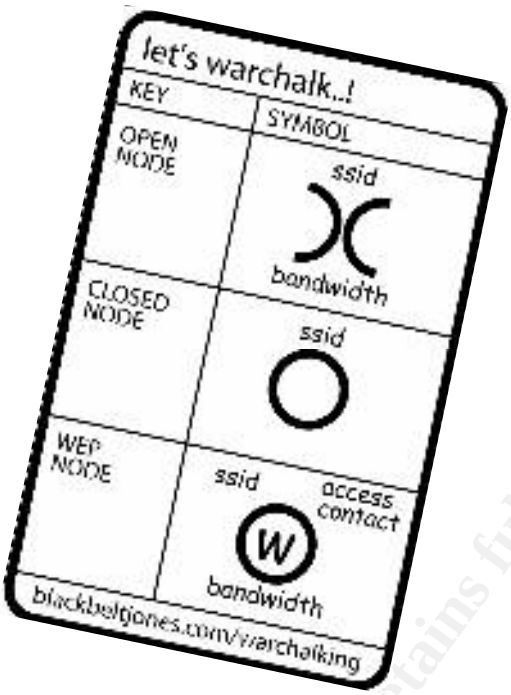
> "Warchalking is the practice of marking a series of symbols on sidewalks and walls to indicate nearby wireless access. That way, other computer users can pop open their laptops and connect to the Internet wirelessly."

The following symbols are used in the “art” of warchalking: [4]

(a) open node

(b) closed node

(c) WEP node



Eavesdropping is another external threat to a wireless LAN. Since wireless LAN uses radio waves, eavesdropping is possible by simply listening to or sniffing the airwaves. When information is sent across the airwaves in an unencrypted state, it is easy for "listeners" to pick up sensitive data such as passwords. Some people use WEP to provide data encryption. Unfortunately, this is easily decrypted and does little to prevent this form of attack. [5]

Man in the middle attacks occur when a hacker sends out a stronger signal than the access point to a user, fooling the user into believing that the hacker is actually the access point and that the actual access point signal is simply an echo. The user associates with the hacker and the hacker associates with the access point. The user then provides authentication information to the hacker, who then provides this to the access point. The hacker is essentially the middle step in the communication process between the user and the access point and has information to everything that passes between them. [6]

Wireless LANs are open to the same security threats as wired LAN infrastructures as well as even some more. It is essential that a company, which has decided to go ahead and deploy a wireless LAN, is aware of these threats and also the methods involved in eradicating them.

Threat Reducing Products

In recent years companies have become increasingly aware of the threat posed to them by the introduction of wireless networks. However, instead of totally

banning these type of networks from business use, much research has gone into finding ways of securing them, resulting in companies embracing the technology. There are many products currently available on the market. Some of these will now be discussed.

NetStumbler is a free and relatively simple tool that provides for the detection of rogue access points. In order to run this software it is essential to have at least a notebook and a wireless LAN card that NetStumbler supports. NetStumbler scans the airwaves for access point beacons and logs them to a file along with any other information, which the access point makes publicly available. Network administrators can analyse these files and determine if there are any rogue access points on their network. It must be noted that NetStumbler only listens for the access point's beacon broadcast, if this is deactivated, NetStumbler will not detect the AP. Most enterprise class devices have this deactivation option, but usually rogue access points are only home networking devices. This software can also be used to discover access points belonging to foreign networks whose signal may be bleeding into your office space. [7]

MiniStumbler is the pocket version of NetStumbler and runs on hand held devices such as the Compaq iPAQ. Hand held devices have an advantage over typically bulky laptops as they can run the tool without being visible to employees. The signal strength can also be used to home in on rogue access points.

Rappore Shield from Rappore Technologies is software that protects laptops and users from accidental association to other ad hoc machines or foreign networks. This software allows users to customise their network and security settings based upon their location. For example, if the user is in a public Internet café, the software can detect this and impose the necessary security restrictions, i.e. not allow ad hoc connections, insist upon VPN connection, insist upon the necessary level of encryption etc. Rappore shield only runs on Windows 2000 and Windows XP. [8]

Red Alert is a network device that constantly analyses the air space around the network and will alert network administration as soon as anything untoward seems to be happening. This box is provided by a company called Red-M as essentially a wireless intrusion detection device. Red Alert is available as power over Ethernet, which allows it to be placed in more remote and secure areas without the need for a power supply or battery. This is beneficial as the device may be hidden from view reducing the chances of it being tampered with. It can be connected to and configured using a browser interface from the network administrator's pc. Red Alert has a feature that allows the network administrator to store records of wireless events and perform an audit trail. From this, the administrator can deduce for example, if there are rogue access points on certain days of the week, this points to the culprit only being in the office on particular

days and makes him easier to catch. Red Alert has a range of 45,000 square feet that facilitates its use in most office environments. [9]

It is essential that all wireless networks be protected in order to ensure the safety of the network in which they are employed. Security can be implemented on the user machines in the form of 3rd party software. It can be implemented on the network itself in the form of intrusion detection devices such as Red-Alert. It can also be implemented on the level of the access point itself. The access point must be configured correctly and installed in a secure location to prevent mischievous hands from tampering with it.

Security Realms

There are several security areas or realms that every company should look at before implementing a wireless network. They are:

- Security Policy
- Physical Security
- Authentication
- Access Control
- Audit and Monitoring

Each of these will now be looked at in greater detail, to show how they each affect the security of wireless networks.

The security policy indicates a company's overall attitude towards security. Even if there are currently no policies for wireless networking in place, existing schemes will determine some of the WLAN security architecture. The following policies, for example, should already be in place,

Physical security of networking devices – this will provide the basis for the policy on WLAN infrastructure devices, ranging from their actual location to who has access to them

Authentication and Encryption – most companies already have policies in place with regards to methods of authentication and what level of encryption must be used when remotely accessing the company network.

Audit and monitoring – corporate networks are monitored to a pre-determined level, ensuring the requirements outlined in the security policy are satisfied. These ideologies will provide the requirements for wireless network monitoring

and allow for decisions to be made as to what type of devices will be used – eg. Red-M.

Although the above-mentioned security policies may already exist for wired networking, they will need to be modified to accommodate Wireless LAN specific issues. It is essential that every company acknowledges that wireless LAN is different from wired networking and must have its own security policies, based upon but different to that of the wired infrastructure.

The WLAN physical security policy should cover the issue of the visibility of wireless devices. Are they physically secured? Can they easily be reached? Is there access to the console port? Who should have access to the console port? Is there access to the Ethernet port? Some companies may wish to keep access points out of sight and all ports physically secured. They may wish to keep intrusion detection devices hidden in order that employees and visitors aren't aware of the fact the air space is being monitored. However, other companies may wish to keep all these devices on display, such as Cisco or Red-M. This would let visitors know that a wireless LAN is available in particular areas and it would also work as an advertisement for the company products.
Wireless device security enclosures are available on the market. These enclosures allow for the antenna to escape via a hole in the enclosure, but at the same time, restricting access to the other components of the device.

Wireless LAN Authentication policy is a must. It is not a question of should there be a requirement for authentication, but instead how will authentication be accomplished? It may be desirable to use authentication methods which are currently in place for the wired LAN; Radius, TACACS, LDAP. This would ensure a centralized scheme and increase ease of management. It may also be desirable to provide extra authentication devices to enhance security further, although, this would increase cost of management. Devices such as Vernier, BlueSocket or Funk may be used for this purpose. There are many things to be considered for the authentication policy, however, it is essential that these be covered.

The Access Control policy will concentrate on issues such as who will have access to the wireless LAN. Should there be a guest account for use by visitors? If so, then the guest account may have limited access to network resources, only to the Internet perhaps. There may be secure zones set up and different groups created. This would ensure that business critical devices are protected from malicious use of the wireless LAN.

The Audit and Monitoring policy must advise what is to be audited. The access point configuration should be regularly audited to ensure that there have been no resets of the device as well as any unauthorised changes. There should be change control processes in place for APs as well as separate administrator accounts for different administrators. Possible AP security configuration changes

include disabling telnet and changing the default http port. There must be regular audits in order that rogue access points can be detected and removed. This policy needs to identify the type of monitoring required by the company. Regular, constant monitoring or periodic monitoring? 24 x 7 continuous monitoring requires the purchase and management of dedicated monitoring radios. This can lead to a great increase in wireless LAN costs. However, periodic monitoring can require manual walk-arounds of the network administrator using software such as NetStumbler. This may result in rogue access points and unauthorised ad-hoc networks being missed.

802.11b Security

Believe it or not, 802.11b security is actually not so secure. The following points will now be discussed,

- Service set identifier (SSID)
- Open authentication
- Shared Key Authentication
- Wired Equivalency Privacy (WEP)

The SSID is a 32 ASCII character string. It is used to differentiate one wireless network from another and segment users and access points which make up the wireless subsystem. The SSID is sent in clear text in the access point beacon frame. This information can easily be seen using NetStumbler or AirSnort, which are both readily available from the Internet. Under 802.11, any client with a null string configured will associate to any access point regardless of the access point SSID, for example, in the case of a client using WindowsXP. Contrary to popular belief, this is most definitely not a security feature.

802.11b devices have open authentication, i.e. all requests are granted. Extra authentication devices are required on the network. If WEP is not enabled, and extra authentication devices have not been employed, the network is wide opened. If WEP has been enabled then it becomes an indirect authenticator and this is most definitely not desirable.

Shared key authentication means that the client and access point have pre-shared keys. The process involves the client initially requesting the shared key authentication. The access point then sends back a plain text challenge, which the client responds to by sending back the challenge encrypted using the WEP key. If the access point can decrypt the challenge then the client is authenticated.

WEP stands for wired equivalency privacy – NOT wireless encryption protocol, which is what many newcomers to wireless often believe. This misconception often results in the false conclusion that by simply enabling and configuring WEP is a satisfactory way of securing a wireless network. It most definitely is not! WEP encryption is based upon the RC4 algorithm. It is optional to use a 40 or 64 bit key, however, some vendors now offer a 128 bit key option. The requirements for Wi-Fi are only 40bit. WEP has many shortcomings, some of which include the fact that the key is too short to resist brute force attacks. WEP only provides for one-way authentication, i.e. the client is authenticated by the access point, but the access point is not authenticated by the client. This can lead to man-in-the middle attacks. WEP cracking tools are readily available on the Internet, eg. WepCrack and AirSnort. WEP should be viewed as equivalent to plugging an Ethernet cable into a laptop to provide a means of connection to a network. It does not provide security.

Conclusion

Wireless networks can benefit the business world greatly. The technology is constantly changing and improving. However, vulnerabilities are continually being discovered and exploited by hackers, whose methods are becoming increasingly sophisticated. This paper has described vulnerabilities which wireless networks may be prone to, as well as products that can satisfactorily secure the network from mischievous eyes. It is important to remember that although wireless network infrastructures are open to security holes, it is still possible to make them as secure if not more secure than the wired network.

References

The following resources have been used in the research for this paper.

[1] http://www.wi-fiplanet.com/tutorials/article.php/2200071

[2] http://isp-planet.com/fixed_wireless/business/2003/rogues.html

[3] http://www.giac.org/practical/GSEC/Rafidah_Abdul_Hamid_GSEC.pdf (P6, section 2.1)

[4] http://www.warchalking.org/

[5] http://www.giac.org/practical/GSEC/Rafidah_Abdul_Hamid_GSEC.pdf (P7, section 2.3)

[6] http://www.wi-fiplanet.com/tutorials/article.php/1457211

[7] http://www.netstumbler.com/modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=Official+NetStumbler+Version+0.3+FAQ

[8] http://www.networkmagazine.com/article/NMG20021203S0005

[9] http://www.red-m.com/Products/pdfs/Red-AlertDatasheet.pdf