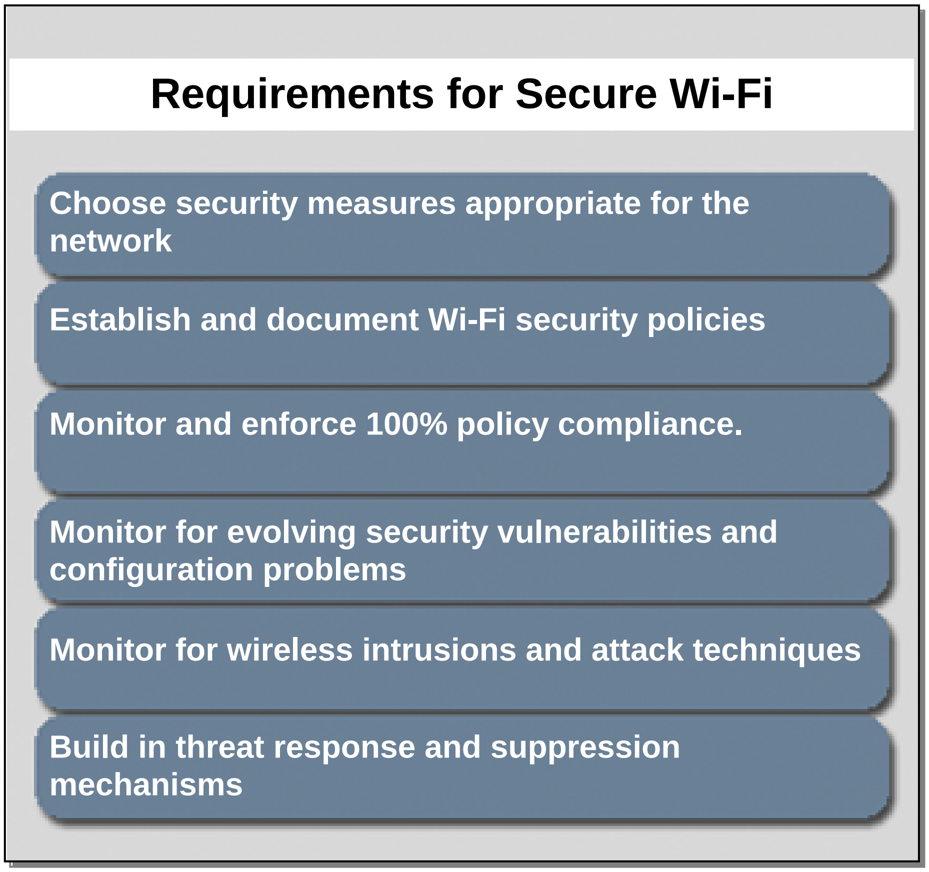
Best Practices for Securing Your WLAN

AIRMAGNET

Table of Contents

Introduction

The steady growth of Wi-Fi in the enterprise demands that corporate IT teams learn and adopt new security methodologies tailored to the unique requirements and weaknesses of wireless networks. Network and security staff must first evaluate a potentially confusing set of authentication and encryption mechanisms to be used in the network. Depending on the security selected, IT will then need to establish and document the corporate WLAN security policy, including mechanisms to validate user compliance and monitor for inherent network vulnerabilities. With a defined policy in place, IT staff can turn their attentions to protecting the network from snooping and an ever-expanding list of wireless attacks. In this paper, we will address each of these areas in detail and identify the real-world best practices needed to deploy and maintain a secure wireless network.



Requirements for Secure Wi-Fi

- Choose security measures appropriate for the network
- Establish and document Wi-Fi security policies
- Monitor and enforce 100% policy compliance.
- Monitor for evolving security vulnerabilities and configuration problems
- Monitor for wireless intrusions and attack techniques
- Build in threat response and suppression mechanisms

Security Policy and Enforcement

Authentication and Encryption are fundamental requirements.

Like any network, WLANs have fundamental requirements in regard to security. At the most basic level wireless security requires Authentication (only authorized users can access the network) and Encryption (information passed on the network can be read only by the intended recipient and without tampering). Much of the confusion relating to wireless security stems from the jumble of protocols that have been proposed to deliver these basic tenants of security. In this section we will take a close look at the most common security methods available today and spell out the strengths, weaknesses, and management issues associated with each. Keep in mind that choosing a security strategy is only half the battle. Insuring 100% compliance with that policy is an ongoing task, and every security strategy carries with it certain vulnerabilities that must be identified and managed by network professionals on a daily basis.

Security choices are independent of 802.11a/b/g choices.

A Note on the 802.11 Standards

The evolution of wireless security has come with new standards, acronyms, and industry jargon that can be difficult to navigate. An important point to keep in mind is that all of the security measures covered in this document will apply equally to a wireless network regardless of whether it is a 802.11a, b, or g network. For all practical purposes the 11a, b, and g standards describe how data is transmitted at the physical level – this is analogous to the copper wire in a wired network. All the other standards and protocols we will discuss run on the layers above this physical layer. For example 802.11i describes a collection of security protocols for delivering strong security on a wireless network. 802.11i can be implemented regardless of whether the network is 11b, 11a, or 11g at the physical layer. Some security methods may have certain hardware requirements in terms of processing power or memory, but once again this independent of the 802.11 standard you choose.

WEP - Wired Equivalency Privacy

- *Authentication* – 1-Sided
- *Encryption* – Weak Implementation of RC4
- *Weaknesses* – Static keys, keys can be broken, highly susceptible to a variety of Man-in-the-middle attacks and session hijacks.

WEP represents the initial attempt at providing wireless networks with a level of security comparable to that of wired networks. In this regard, the standard has proven to be a failure due to an abundance of widely publicized vulnerabilities. Understanding of these weaknesses is key, because they have had a great impact on the security strategies that have evolved to replace WEP.

One set of keys for the entire network.

WEP's failures can be traced back to a few specific fatal flaws. First, WEP encrypts traffic using a single pair of keys that is shared among all users on the network. This means that if the keys are compromised, the entire network is compromised. To make matters worse, changing keys is typically a manual process that must be carried out on a client by client basis.

24-bit IV means that IVs are re-used.

Secondly, every WEP encrypted packet uses of a 24-bit counter called an Initialization Vector or IV. The idea is that since each packet has a different "random" IV, then it would much more difficult for a hacker to discover the key. The weakness comes from the fact that since this the IV is only 24 bits in length, there are a limited number of IVs available. Since each individual packet gets its own IV, all the possible IVs are quickly exhausted in a normal network. This allows someone snooping the network to capture wireless packets with the same IV, and then use easily available tools such as AirSnort to break the keys and view the packet contents in the clear. This is of course constitutes a complete failure of security.

One-sided Authentication doesn't protect the client.

The final major WEP weakness stems from the fact it only requires a 1-sided authentication, meaning that the Client must authenticate itself to the AP, but the AP does not authenticate itself to the client. Thus an attacker can easily pretend to be an approved AP, and when an unsuspecting client associates to this attacker AP, that client has no way of knowing that the AP is an imposter. At this point the attacker can gain a great deal of information about the client and even impersonate that client to an approved AP.

Even with these weaknesses it is important to keep in mind that using WEP is certainly better than using nothing at all. At the very least it is a readily available solution that clearly denotes a private network, and as such will discourage most war-drivers. Given the abundance of WLANs with absolutely no security whatsoever, most snoops will see a WEP-protected network and move along looking for an easier target. The hacks described above while well documented, do require a certain degree of expertise and many war-drivers are relatively benign snoops simply looking for free internet access.

More reading: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

802.1x = Authentication ONLY

- *Authentication* - 2-sided (in most cases)
- *Encryption* – None; Used in conjunction with an additional security mechanism.
- *Weaknesses* - Many methods of using 802.1x, some require a certificate, some are vulnerable to dictionary attack.

802.1x provides strong authentication and a platform for delivering new keys

When the weaknesses of WEP were identified, industry professionals were forced to scramble for solutions, and one of the best to arise was 802.1x. 802.1x provides a way to leverage traditional strong authentication mechanisms such as a RADIUS server in a wireless network. In such a scenario the client must authenticate itself to the RADIUS server, and the AP authenticate itself to the client before either granted access to the larger network. In addition, 802.1x can be used to automatically deliver new keys to a client and AP dynamically, thus overcoming the static key weakness of WEP. In this regard, 802.1x is sometimes referred to as dynamic WEP. This is a bit of misnomer, because as we will see, 802.1x can be used in conjunction with many other types of encryption.

EAP is the important component of 802.1x, and many EAP options are available.

To deliver these services, 802.1x implementations must use one of several authentication protocols called EAP types (Extensible Authentication Protocol). EAP is responsible for establishing how the authentication process should be carried out. This establishes the rules so that both client and AP know the rules and appropriate responses for a successful authentication. The most popular EAP types are LEAP, PEAP, TTLS, and Cisco's FAST. Each of these methods has their own unique strengths and considerations, and choosing the correct method for your network can be one of the most important steps of the security design process. The table below provides a brief overall comparison of the various EAP types.

EAP Type	Client Certificate?	2-Way Authentication	Susceptible to Dictionary Attack?
MD5	Password	No	Yes
LEAP	Password	Yes	Yes
TLS	Yes	Yes	No
PEAP	No	Yes	No
TTLS	No	Yes	No
FAST	No	Yes	No

MD5 – This is the weakest of the possible EAP methods and typically should not be employed in a WLAN inasmuch as it provides negligible benefits over WEP.

LEAP – Provides an easy way to get 2-way authentication without using certificates. The weakness is that it requires users to remember a user password, and is thus susceptible to dictionary attacks.

TLS – Provides a very secure solution, but requires the use of certificates on the client.

PEAP – Very secure solution. Uses TLS to create a secure tunnel where a second authentication mechanism can be used. Does not require a cert on the client, but will use a cert on the server.

TTLS – Very secure solution. Very similar to PEAP; Uses TLS to create a tunnel to avoid using certs on the client.

FAST – Very secure. Creates a secure tunnel, then uses AAA server to authenticate the server and client.

Keep in mind that 802.1x is a necessary part of a strong security solution and does not exclude other security measures. 802.1x will address authentication, but must be coupled with an encryption strategy as well. For example, 802.1x is used a component of both WPA and 802.11i, and not an alternative.

WPA and 802.11i

- *Authentication* - 2-sided provided by 802.1x
- *Encryption* – Strong
- *Weaknesses* – Security itself is very strong. Must be properly managed.

Similar standards from separate standards bodies.

Both use 802.1x

WPA and 802.11i are intimately related standards in terms of their composition and how they work. Keep in mind that neither WPA nor 802.11i are not the security mechanisms themselves, but simply a name for a collection of specific security protocols. Both standards rely on 802.1x to provide strong authentication. Both standards then apply strong encryption mechanisms to serve as a complete replacement for WEP. So why the need for two standards with such dissimilar names? In short, because they come from two different standards bodies with different time lines. 802.11i is the standard proposed by the IEEE, and is the official standard to replace WEP. WPA is the standard delivered by the Wi-Fi Alliance as a solution that could be used immediately while 802.11i goes through the long process of ratification. Once again these terms are not mutually exclusive as WPA is designed to be forward compatible with 802.11i.

WPA uses TKIP for encryption.

The key difference between the two standards revolves around the encryption mechanism used in each. WPA replaces the WEP encryption with a protocol called TKIP. TKIP, like WEP uses the RC4 cipher but in a much more secure way. Namely, TKIP uses a 48 bit Initialization Vector (IV) as opposed to the 24 bit IV used in WEP, and automatically change keys after a specified number of packets. This provides a very strong level of security in a solution that can be deployed today.

802.11i uses CCMP for encryption.

802.11i is virtually identical to WPA, except it specifies the use of CCMP for encryption instead of TKIP. CCMP makes use of the AES cipher and is typically considered the most robust encryption strategy available. The trade-off is that AES requires additional processing power and may not be supported by older hardware. 802.11i is scheduled for ratification in June of 2004. To keep WPA up to speed with 802.11i, the Wi-Fi Alliance is planning to release a second version of its standard called WPA2, which will map directly to the 802.11i standard.

Standard Name	WEP	WPA	802.11i / WPA2
Encryption Name	WEP	TKIP	CCMP
Cipher	RC4 40 or 128 bit 24 bit IV	RC4 128 bit 48 bit IV	AES 128 bit 48 bit IV

VPN

Trusted solution that is readily available, but difficult to manage

VPNs have been and remain a standard security practice for providing secure access from an unsecure or non-trusted location. In this regard, VPNs make a good deal of sense for use in wireless LANs, and many network managers have taken this approach. The main advantage of the VPN approach is that it leverages technology and skills that many IT managers already possess and is vendor neutral in terms of access points. This means that it is deployable today with very little learning curve. The drawback is that it requires management effort on each wireless client, which can quickly become unmanageable if Wi-Fi is to be rolled out to all employees and network users. Additionally, VPNs come with significant processing requirements that could negatively impact the overall performance and scalability of the network. It is also worth noting that a VPN solution only begins working at Layer 3, whereas the other security methods discussed above work at Layer 2. As a result, VPNs are typically best suited for smaller wireless deployments. As the network grows to support more users, IT want to plan a migration to a more scalable enterprise-wide approach to security.

Compliance and Vulnerability Testing

A secure network is the result of an ongoing security process and not simply the installation of security technology. This means that even with a strong security strategy in place, IT must also actively monitor and enforce compliance with that policy, and be aware of the vulnerabilities inherent in the strategy they have chosen.

Compliance requires visibility into every device in the network

Policy compliance requires an awareness of the configuration of every AP and client in the network including the security measures employed on each. This is easier said than done as more and more wireless-ready PCs are shipped with little to no security in place. For example, a typical laptop PC may have both an internal and an external wireless card, either of which could create a vulnerability to the network if not properly configured. This problem requires a monitoring system that is capable of detecting any and all wireless devices in the area of the network. An advanced system, such as AirMagnet, allows IT to specify a detailed security policy tailored to specific wireless resources and then generate automatic alerts when the policy is violated.

Even the most secure systems have vulnerabilities

In addition to compliance, every security solution no matter how strong requires regular monitoring for inherent weaknesses and vulnerabilities. For example, even in a WPA installation, IT needs to verify the system is not running in Pre-shared Key Mode which can cause serious vulnerabilities. Networks running 802.1x must be monitored to insure proper rekey timeouts are adhered to, and multicast and broadcast traffic are encrypted properly. Furthermore, a variety of configuration issues must be addressed such APs broadcasting their SSID, clients operating in ad-hoc mode, or clients with open WLAN connections. These are just a few examples and it is important to realize that every security implementation requires regular attention and it is up to IT to learn the vulnerabilities of their security strategy and deploy solutions that can monitor for them.

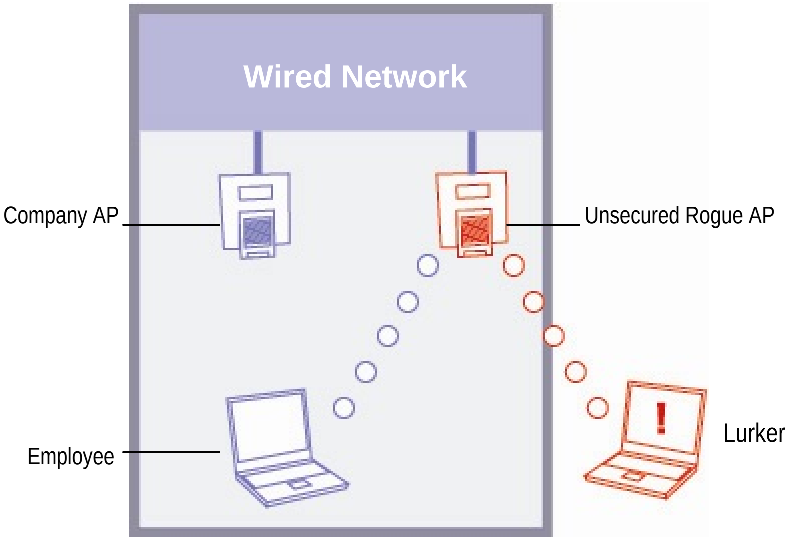
Wireless Intrusion Detection and Prevention

With the network's basic defenses deployed and maintained, technical teams can shift their attention to the subject of defending the network from attacks. Attacks can come in a variety of forms, and in many cases can even be unintentional. Wireless LANs by their very nature provide a way of accessing the network through walls and physical barriers that normally protect business assets. Add this to the fact that most WLANs are not properly secured, and it is no wonder that an intruder would look to the wireless network as the ideal place to begin an attack.

Rogue Detection and Prevention

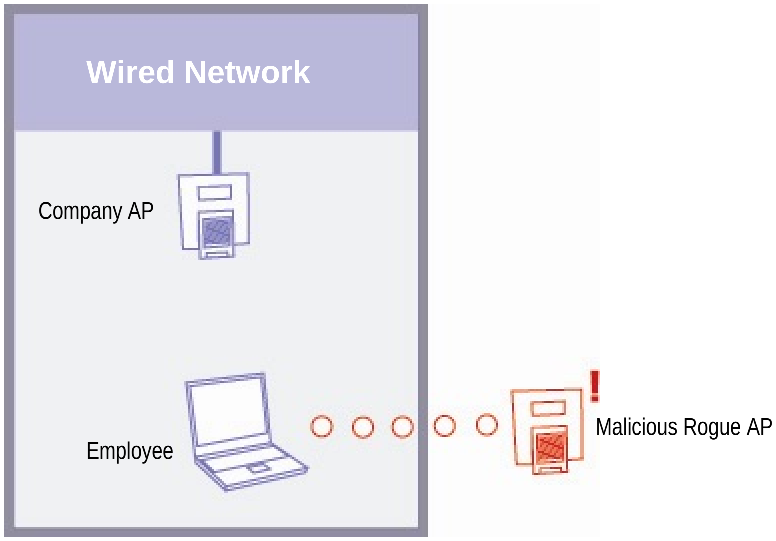
The problem of rogue access points has garnered more attention in the industry than any other security issue, and for good reason. A rogue access point is any access point in your network that was not intentionally deployed by your network staff. They can come from well-meaning employees who bring in devices from home, they can be devices used by attackers for malicious purposes, or they can be neighboring devices that simply overlap with your wireless network. These devices can have many effects and none of them are good in terms of network security.

The most common rogue AP scenario involves devices introduced by employees. In this case, the employee brings in an unsecured access point, plugs it in to an available wired port and now has wireless access to the larger wired network. Unfortunately, so does anyone else within range of the access point including the wireless lurker in the parking lot. This provides virtually unchecked access to the entire enterprise network.



Unsecured Rogue Access Point Allows Anyone to Connect to the Network

An attacker could pursue the strategy described above by planting a rogue device inside the building. However in many cases the attacker may not have physical access to the site, so he or she will use a rogue AP as part of a more sophisticated attack. In this case, an attacker would set up a rogue AP outside the building in an attempt to lure a client into mistakenly associating with it. When this happens, the attacker is free to obtain data from that client directly and can also gain information such as the client's login info and credentials which the attacker could use at a later time.



Malicious Rogue AP Used to Lure Employees Away From the Enterprise Network

Rogue detection must address stations as well as APs

While the focus thus far has been on access points, the same principles also apply to clients. A rogue client could indicate an unknown user trying to get unauthorized access to the network. On the other hand, it could be an unconfigured employee device searching randomly for any available connection. In either case it represents an issue that requires immediate attention from technical staff.

Rogue detection requires defined policies and continuous monitoring

The solution to the issue of rogue devices will always begin with detection. Fundamentally, security staff needs to have complete visibility of every access point and client in the network coupled with clear cut rules that identify the devices that are authorized to be in the network. The more specific the wireless policy, the easier rogue detection becomes. For example, if you know the MAC address of your devices, you can then easily identify rogues based on MAC address. In the same way, Rogues can also be identified based on other factors such as the hardware vendor, Channel, or SSID. All of this requires the ability to scan the airwaves and identify each and every device based on a variety of criteria, again illustrating the need for comprehensive wireless monitoring.

As a closing note, it is important to think of rogue detection as part of the larger security policy and not the security policy itself. Rogue APs have been so well covered in the media that the tendency is to think of rogue detection and wireless security as the same thing. This puts the cart before the horse inasmuch as it addresses the most publicized issue but ignores the hundreds of issues and weaknesses that sophisticated attackers would exploit.

Rogue Suppression and Response

Any rogue device should be considered a threat to the network and requires a set of responses on the part of network staff and security systems. The response process should ideally be broken to two phases – a suppression phase where the rogue device is immediately quarantined from the network, and a removal phase where the device is physically located by staff and potentially removed from the network.

Rogue Suppression

When a rogue is detected, the first order of business is to limit its access to other wireless devices in your network and especially to the larger wired network. This can be done using blocking strategies that typically fall in one of two broad categories – wireside blocking and wireless blocking.

Wireside blocking techniques seek to block rogues at the point they reach the wired network, namely at the port or the switch. This provides strong protection for the wired LAN and should be strongly considered as part of multi-layered approach to rogue suppression.

Rogue Suppression can include a mix of wired and wireless blocking techniques

Wireless blocking involves the use of a separate wireless security device to block the rogue from making any connections on the wireless side. This is performed through a variety of methods, but the end goal is to insure that the device cannot make outbound connections to other devices and devices cannot make inbound connections to it. This ability to quarantine is of particular importance when you revisit the rogue scenarios discussed in the previous section. Recall that in many cases the rogue may not even be plugged in to the wired LAN. A malicious rogue user may attempt to lure clients to his AP as part of a larger attack on the network. Without the ability to block in the wireless domain, IT is essentially powerless to stop these attacks. Additionally, since wireless blocking suppresses the rogue at the source, it also provides additional protection to the wired network.

Physical Response

Physical response is the only long term solution for rogue suppression

After a rogue device is quarantined a physical response to remove or reconfigure the device is still required. All blocking techniques, whether wireside or wireless, will have some level of impact on the performance of the network. Shutting down a port obviously removes that port from use in the network, and is not a strategy that could be pursued indefinitely. Wireless blocking requires the blocking device to regularly send blocking messages to the rogue device, which will result in the rogue repeatedly failing in its connection attempts. All of these messages constitute traffic on the WLAN that is essentially doing nothing in terms of the core function of the network, which is communication. While the effect of this process is negligible in individual cases, it doesn't make sense to incur this overhead on a large scale when the rogue can be removed.

To remove a rogue device, IT will need to be able to locate it in space, and this will require specialized tools designed for the task. Tools such as the AirMagnet Laptop and AirMagnet Handheld analyzers provide 'Find' tools that allow IT to lock in on a rogue's MAC address and track down the physical location of the device. This provides IT with the ability to pull the device out of the network and potentially meet its owner face-to-face. If the rogue has been brought in by an employee, you will want the opportunity to explain the security policy as well as get an understanding of the reasons why the user brought the device in the first place. Perhaps he or she has poor coverage from the corporate WLAN and was trying to solve a problem.

Network Snooping

Basic tools allow hackers to collect info, even from secure networks

Wireless eavesdropping is perhaps the most fundamental technique available to wireless hackers and hobbyists. Popularly referred to as "war-driving" or "war chalking", this practice refers to the use of basic wireless tools to passively listen to wireless conversations to gain information about the network. The most common tools such as NetStumbler and Wellenreiter are easily available and in widespread use. In its most benign form this can be a simple way for a user to find free wireless access or hot-spots. Alternately, hackers can scan the network to find security vulnerabilities or collect data to mount an attack on the network.

Although difficult, it is possible to detect these probing devices

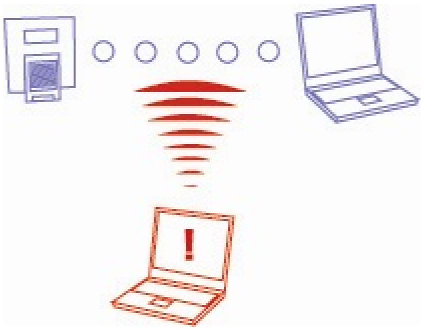
While it is notoriously difficult to detect devices that are snooping a WLAN, it is not impossible. Typically, each of these scanning tools will probe the network in a unique way, and this probing method can serve as a signature for that particular tool. The difficulty lies in the fact that they send out very few packets, and as a result there are limited opportunities to identify them. This underscores the importance of having a dedicated monitoring system that captures as many packets as possible, covering all channels, bands and devices.

MAC Address Spoofing

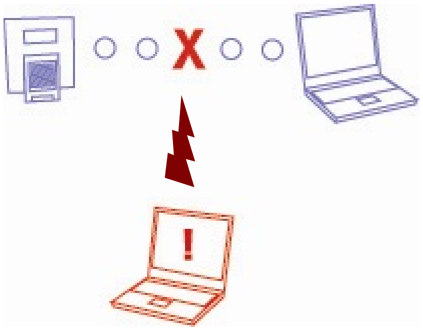
Network managers must address a host of wireless intrusion techniques beyond rogue devices, and MAC address spoofing may be at the top of the list. Since every network device in the world is issued its own unique MAC address, it makes sense that network managers use these addresses to identify the devices on their network. As we have seen before, MAC addresses are one of the most common ways of distinguishing between devices that are authorized to be on the network and those that are rogues. The problem arises because simple software and techniques are available that allow an attacker to send out packets that appear to come from any MAC address the attacker chooses. This means the attacker can snoop traffic on the network, identify an approved client's real MAC address, and then pretend to be that device.

MAC Spoofing is a fundamental part of many attacks

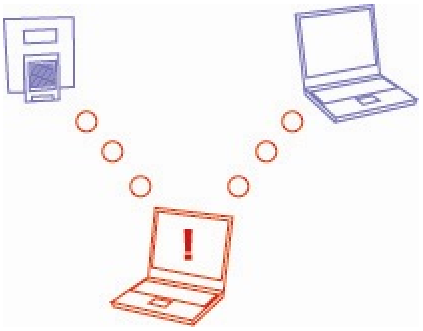
This technique is a fundamental component in a variety of sophisticated attacks such as Man-in-the-Middle attacks and Session Hijacking. The Man-in-the-Middle attack relies on the attacker fooling an access point into believing that the attacker is an authorized client, and fooling the client into believing that he is the access point. If the attacker succeeds at this ruse, then he is effectively intercepting all traffic between the client and AP without their knowledge.



1. The attacker monitors both the AP and Client, picking up their MAC Addresses and authentication information in the process



2. The attacker breaks the connection between the AP and client. (Denial of Service attacks covered later).



3. Attacker spoofs MAC addresses to fool both the AP and client into connecting to him.

This is a bit of an oversimplification of the process, but the ability to deceive both the AP and client is the essential component of the attack, and MAC address spoofing is a key component of how this is done.

IT teams have several options to help them combat MAC address spoofing. The first line of defense is to consider implementing a security policy that mutually authenticates both sides of the wireless conversation using methods more secure than the MAC address. This would mean moving to an 802.1x based authentication scheme that uses EAP-TLS or better.

Best strategy to fight spoofing includes strong security measures and direct monitoring

Additionally, management teams will want to monitor directly for devices that are spoofing MAC addresses in the network. Advanced wireless monitoring systems can detect spoofed MAC addresses using multiple methods. First, devices will retain a wireless "fingerprint" that is unique to each manufacturer. Likewise, MAC addresses can be traced back to an individual manufacturer. This means that the monitoring system can identify devices that are announcing a MAC address that is different from the actual hardware they are using.

Additionally, a stateful monitoring solution will be able to track all packets from all sources. If an unusual number of packets from the same MAC address are detected out of sequence, this could be a sign that two devices are operating with the same MAC address. When an attacker is detected spoofing another user's MAC address, network managers can use the same blocking mechanisms used to suppress rogue devices.

Denial of Service

DoS Attacks can target any level of the network depending on the goal of the attack

Denial of Service (DoS) attacks represent yet another threat to the wireless infrastructure. A denial of service attack overloads some aspect of the wireless infrastructure, effectively removing it from the network. Such an attack can be launched against a specific station, access point or can target an entire network depending the attacker's goals. For example, if an attacker wanted to shut down an entire WLAN, he or she could attempt to flood the RF spectrum itself to paralyze the entire WLAN. On the other hand, an attack may be targeted to one particular device as part of a larger attack. For example, if we revisit the Man-in-the-Middle attack. A common technique is to find a connected AP-client pair, then break the connection between the AP and client using a denial of service technique.

Denial of service attacks can come in a variety of forms. At the most rudimentary level, an attacker can disrupt wireless communications by flooding the 802.11 spectrum with an excess of noise. This technique is typically referred to as RF Jamming and makes wireless communication either impossible or highly unreliable.

Other more sophisticated DoS attacks attempt to exploit various 802.11 rules or hardware limitations to overwhelm a particular device. For example, most APs have a set limit of stations that can the AP can support. An attacker can use this information to attack the AP by flooding the AP with more associations than device can process. In much the same way, the attacker may try to overoad a specific step of the association/authentication process. Regardless of the unique methodology, the result is the same – an inoperable device and a weakened network.

Many types of DoS attacks exist, each with a unique signature

To detect these attacks is of paramount importance to have a dedicated wireless monitoring system that is separate from the communication infrastructure. If an access point is serving clients in the network, then one must assume that an attacker can snoop this traffic and acquire the basic information needed to attack the AP. This illustrates the logical need for monitoring that is independent of the regular network infrastructure. Additionally, given the rapid evolution of denial of service attacks in both number and sophistication, timely and dedicated expertise is required to recognize the unique signature of each attack.

Miscellaneous Threats

Wireless LANs face an ever-growing list of attacks in addition to the techniques listed above. While it is beyond the scope of this document to provide an exhaustive list of them all, it is important to be aware of the more common attacks. These include:

Dictionary Attacks

Dictionary attacks involve brute force attacks on user passwords

Dictionary attacks target any authentication mechanism that relies on a human entering a user name and password to verify their identity. LEAP is the most common example. The attack takes advantage of the fact that when choosing a password, most people will pick a word that it is easy for them to remember. Hackers have recognized this human tendency and built a list or “dictionary” of the most common passwords and their variants. Since the user name can be captured by snooping traffic, the attacker needs only to guess the password. The attacker will then use software to quickly attempt to authenticate using every word in his dictionary until the correct password is discovered. The strength of this attack stems from the fact that the attacker doesn’t really need any detailed information about the network. He or she can potentially sit comfortably in the parking lot and figuratively try every key on every door until a match is found.

These attacks can be countered in two ways. First, management should enforce strong password policies for all network users. This means users should use passwords that are of substantial length (8-10 characters), include numeric characters, and use both upper and lower-case letters. The second response is to monitor for these attacks directly. A wireless monitoring system will be able to detect a station that is constantly and repeatedly failing in its authentication attempts. This behavior should generate an alarm for the network staff, who can then choose to block the device or track it down with a mobile analysis tool.

Soft APs

Soft APs could probably be lumped into the larger category of rogue devices, but are becoming so prevalent that they deserve their own category. A soft AP refers to the use of specialized software to convert a regular laptop or desktop PC into an access point. When this happens, the result is almost always a rogue access point. This ability is of particular significance as they represent a tool of choice for WLAN hackers when launching an attack. For example, if an individual wanted to launch a Man-in-the-Middle attack or Denial of Service attack, it is far more practical (and inconspicuous) to use a laptop instead of carrying around an actual AP. For this reason alone it is of critical importance to be able to scan for and detect soft access points. Identifying a soft AP can be notoriously difficult to do, and is best almost impossible to do without monitoring software designed for that purpose.

Security Best Practices

The sections above should provide a strong introduction to the security issues and threats posed to today's wireless networks. It should not however be considered an exhaustive list of all the wireless threats known to exist, and new threats will continue to evolve. However, the state of wireless security has matured to the point that networks can be secured and defended using technology and solutions that are readily available and manageable. Every wireless network should adopt an appropriate security policy coupled to a system for monitoring and enforcing that policy. The following is a brief summary of the core pieces of a strong wireless security strategy.

- Select and deploy a security policy for the entire enterprise – The policy should include authentication and encryption measures commensurate with the resources of the network.

- Monitor for 100% compliance of the chosen policy

- Perform regular vulnerability assessment to identify evolving weaknesses in the underlying security implementation.

- Monitor for a broad set of wireless attacks and intrusion techniques – Rogue devices, Denial of Service Attacks, advanced attacks.

- Include measures to respond to and suppress wireless threats

- Comprehensive Monitoring including all 802.11 standards, channels, and infrastructure vendors.

- Include mobile tools that technical teams can employ in the field to track down policy violations and intruders.

The AirMagnet Solutions

AirMagnet provides a family of solutions that were designed from their inception to proactively diagnose and solve the security and performance challenges of wireless networking. This product family includes mobile tools that IT teams can rely on in the field, as well as dedicated monitoring systems that can provide around-the-clock monitoring for any number of wireless LANs spread over any number of locations.

Detection

At the core of these solutions is the industry's most advanced analysis engine, called AirWISE. This engine automatically analyzes any wireless network to proactively identify over 100 security and performance threats. Categories of threats detected include:

- Security
    - Authentication and Encryption Problems
    - Configuration Vulnerabilities
    - Rogue Device Issues
    - Wireless Intrusions
    - Denial of Service Attacks

- Performance
    - RF Management
    - Traffic Analysis
    - Overloaded Hardware and Channels
    - Deployment and Operational Issues
    - 802.11g Issues

Alerting

Each detected threat can generate an alarm configured to the needs of the environment, allowing IT to tailor their monitoring system to a security policy of any level of complexity. Every alarm that is generated comes with a wealth of event-specific explanation and expert advice. This provides IT with both topical technical data as well as the best practices of possible solutions. This provides an environment of proactive detection and response that allows IT to address evolving issues before the network or users are impacted.

Response

In addition to detecting problems and providing network professionals with the key information. AirMagnet provides the ability address problems actively. In terms of security, the AirMagnet Distributed solution provides wireless blocking to quarantine threats and intruders. Likewise, intruders can be traced to locate their presence on the wired network. The mobile solutions include tools that allow IT to physically track down and pinpoint any intruder or policy violation in the network. This provides a level of accuracy that exceeds what can be offered by triangulation and puts staff face to face with a security problem. On the performance side, AirMagnet offers a suite of active tools that can be used to directly pinpoint any number of performance problems and resolve them quickly.

To learn more about our solutions, we encourage you to visit our website at http://www.airmagnet.com.

About AirMagnet

Founded in 2001, AirMagnet, Inc., provides the most trusted WLAN management and security software systems for the enterprise in handheld, laptop and distributed configurations. Used by IT professionals at more than 2,000 companies worldwide in manufacturing, financial, retail, service, health care, utility, transportation, education and government sectors, AirMagnet solves Wi-Fi connection problems, tracks down unauthorized access, simplifies site surveys, and locks in unprecedented levels of network performance, security and reliability. Unlike traditional packet scanners and protocol analyzers that have been adapted from their original purpose to analyze wired networks, AirMagnet solutions were designed specifically for wireless LANs. Additional information about AirMagnet and its products is available on the Web at www.AirMagnet.com .