GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Secure Wireless Networking for the Home Office

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

Option 1 - Research on Topics
in Information Security

Submitted by: Sujeet Bambawale

Paper Abstract:

Wireless networking has enjoyed abundant popularity in the consumer marketplace as a means to allow the easy and unfettered distribution of broadband connectivity within the home or home office. While recent revisions of wireless network protocols have made security one of their main focus areas; these changes have been slow to percolate into the consumer market. Thus, the average home office that uses a wireless network is often at risk of being compromised by attackers using the wireless network as their medium of entry. In addition, home office users are often connected to a corporate network via a VPN or similar remote connection technology, and such attacks on the home network can translate into a risk for the concerned corporate network and data as well.

This paper details the steps necessary to enforce a reasonably high level of security on a wireless network in a home office environment and describes the implementation of an intrusion detection system to automate the monitoring of the wireless network against external threats.

© SANS Institute 2005 Author retains full rights.

Table of Contents

1 Summary 1
2 Introduction 2
2.1 The state of things today 2
2.2 The home office 3
2.3 The wireless network 3
3 Simulating the home office environment 4
3.1 Hardware selection 5
3.1.1 Wireless client adapter hardware 5
3.1.2 The wireless router 5
4 Access control 6
4.1 Customized configurations 7
4.1.1 The Wireless Zero Service in Windows XP 8
4.2 Authentication 12
4.2.1 Two-factor authentication 12
4.3 Logging 13
4.4 Physical security 13
4.5 Automated intrusion detection 14
4.5.1 AirSnare 15
5 Securing the network 17
5.1 Customized configurations 18
5.2 Authentication 24
5.3 Logging 26
5.4 Physical security 28
5.5 Automated intrusion detection 30
6 Potential attacks and countermeasures 33
6.1 Testing the security of the network 34
6.2 Executing the tests 34
6.2.1 Using AirSnort 34
6.2.2 Using the right WEP key but the wrong MAC address 34
6.2.3 Using the right WEP key and the right MAC address 35
7 Conclusion 36
7.1 Comparison against commercial solutions 36
7.2 Salient features 37
7.2.1 Advantages 37
7.2.2 Disadvantages 37
7.2.3 Suggestions to maintain a secure wireless network 37

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

List of Figures

Figure 1: The administrator console showing the SSID-change screen 18
Figure 2: Changing the default network location of the administrator console ... 19
Figure 3: Enabling the in-built firewall functionality 20
Figure 4: Disabling unnecessary server access 21
Figure 5: Disabling the DMZ 22
Figure 6: Enabling restrictive DHCP leasing 23
Figure 7: Enabling WEP and using a HEX key 24
Figure 8: The MAC address filter 25
Figure 9: Configuring the logging feature of the router 26
Figure 10: Examples and analysis of log data 27
Figure 11: Views of an omnidirectional antenna's signal coverage pattern [Diagrams taken from the documentation for the D-Link ANT24-0700 Omni-Directional 7dBi Indoor Antenna; ftp://ftp10.dlink.com/pdfs/products/ANT24-0700/ANT24-0700_ds.pdf] 28
Figure 12: Views of a directional antenna's signal coverage pattern [Diagrams taken from the documentation for the D-Link DWL- M60AT 2.4 GHz Directional Indoor Antenna; ftp://ftp10.dlink.com/pdfs/products/DWL-M60AT/DWL-M60AT_ds.pdf] 29
Figure 13: AirSnare interface 30
Figure 14: AirSnare - Identifying connectivity problems 31
Figure 15: AirSnare's "AirHorn" module 32

© SANS Institute 0 5 Author retains full rights.

© SANS Institute 2005 Author retains full rights.

1 Summary

David M. Ewalt, a technology journalist for Forbes, recently wrote about engineers developing a new technology called the "wireless mesh"[1] which can be best described as a "no strings attached" connection of multiple wireless networks to create one gargantuan wireless network that could span a wider area with the same connection reliability as a single one.

Aside from being an innovative way of extending the benefits of wireless networks to users who cannot maintain proximity to their "home base", of sorts, this effort also indicates the level of interest and effort that wireless networking has attracted over the last couple of years. From organizations with large campuses to entire cities, wireless network deployments are gaining ground and carving a critical niche in society.

However, the downside is that one can no longer depend on the physical perimeter as a means of keeping intruders away from the network. With the growing instances of identity theft and strict regulations concerning access controls being enforced on corporate networks, wireless networks have proven to be double-edged swords that offer increased productivity at the cost of an increased security risk.

Experts in academia and in the networking industry have often made a good case towards the need for robust security in wireless networking technology. While recent revisions in the wireless networking protocol specifications have translated several of these requirements into reality, the average consumer is often known to avoid configuring the security-related settings on wireless networking devices. Such insecure networks owe themselves, in part, to the meager attention paid by most device manuals to a user-friendly explanation of the security settings and features.

This paper will discuss the consumer aspect of wireless networking by simulating an average home office wireless network environment and outlining a series of steps that can be easily implemented to secure it against most common risks, including the use of a wireless intrusion detection system. Through a rudimentary audit using common wireless audit tools, it will describe the resilience of a network protected by these safeguards, against common attacks. In conclusion, this paper will offer the premise that; if implemented correctly, network configurations and security features available in most consumer wireless network hardware can be used to enforce a reasonably high level of security.

[1] See Ewalt.

© SANS Institute 2005 Author retains full rights.

2 Introduction

2.1 The state of things today

There are numerous tools available freely off the Internet [2] that allow for varying degrees of audit capabilities on a wireless network. Their features sets range from the passive detection of wireless access points in the vicinity, to the intrusive injection of dummy packets into a specific wireless network in an effort to cause a denial of service condition. Needless to say, these tools can be of immense help to an audience ranging from the security-conscious network administrator to the malicious attacker.

The availability of such tools on a medium as public as the Internet raises a plethora of concerns, especially when viewed in light of the fact that computer manufacturers, Internet service providers and wireless network hardware vendors have taken the initiative to demystify and drive the concept of wireless networking to the average consumer. As a result, the deployment of wireless networks has seen a startling rise in recent times, and is not limited to commercial use. An increasing number of residences have "gone wireless" to allow everyone in the household the functionality of the Internet while enjoying the portability of the laptop.

However, a wireless home network can often be more than just a means to get online from one's favorite chair across from the fireplace. Most home networks host a significant volume of data that could be of great value to an intruder. Documents containing personally identifiable information and sensitive content in the form of archived personal communication, financial data, identity data and authentication credentials are examples of data that could be misused easily by a malicious outsider towards perpetrating crimes like identity theft, blackmail, etc.

As with most networking technologies in the consumer domain, easy troubleshooting and security safeguards are aspects that are often sidelined by most advertising and user literature. While the devices often have a feature that can support several security measures, users tend to focus on the 'plug and play' part of their home networks, and tend to lose interest in the network once everything is up and running smoothly.

© SANS Institute 05, Author retains full rights.

---

[2] See Bradley.

© SANS Institute 2005 Author retains full rights.

2.2 The home office

Home office environments usually involve between one and five users and an always-on broadband connection to the Internet. In order to protect the data and users connected to the network, wireless network deployments in such environments have to be secured with the right set of access controls. Furthermore, it is not uncommon to see home office environments leverage some flavor of remote access technology in order to connect with an employer's or a business partner's network. In such instances, a compromise of the home office network could cascade into a compromise of the network(s) it is connected to; allowing the attackers a portal to additional confidential data and resources.

2.3 The wireless network

The average consumer wireless network consists of a wireless router, one or more wireless-network-friendly (portable) computers and an always-on broadband connection to the Internet. A multitude of wireless network technologies exist today; grouped under the ubiquitous "802.11" umbrella. The "802.11" nomenclature can be described as an IEEE specification for a family of protocols supporting Wireless Local Area Network technology. Most of these protocols use the 2.4 GHz frequency band for data transmission using either Frequency Hopping Spread Spectrum or Direct Sequence Spread Spectrum protocols.

A wireless router uses one of these protocols to network the computers connected to it and, in most cases, to distribute an always-on broadband connection to the Internet between them. The 802.11g protocol is en route to replacing 802.11b as the protocol of choice used by wireless network hardware vendors in their current line of devices. The 802.11g protocol allows a larger bandwidth to users within the network (to share large files, have more open connections, support more users, etc.) and also incorporates some additional security features that allow the users to easily enforce a high level of security on their networks.

However, 802.11b enjoys considerable usage in the consumer market, especially among those who rode the first wave of wireless networking in the consumer world and aren't willing to upgrade for the increased internal bandwidth and the additional security features. Wireless routers using 802.11b are very common in residential and home office environments, and thus shall be the focus of this study.

This paper shall detail security safeguards that a user can implement on a 802.11b wireless network using configurations and settings available in most wireless network hardware available in the consumer marketplace.

© SANS Institute 2005 Author retains full rights.

3 Simulating the home office environment

The selection of hardware and software for this simulation was intended to approximate a real-world home office environment as closely as possible. To do so, I factored in the following possibilities:

- **A user volume between one and five**

  These users would be authorized long-term users of the wireless network; and would have "standard issue" wireless networking hardware and software; i.e. software and hardware of the same type / vendor / brand as the rest of the users in the user community.

- **A "guest user"**

  This would be an authorized short-term user of the wireless network, and would have non-standard wireless networking hardware and software. "Non-standard" equipment can be briefly described as diverse operating systems, wireless network client hardware, especially those that aren't deployed within this environment on an on-going basis.

- **A vendor-neutral hardware setup**

  There is a common premise that wireless network hardware that is manufactured by the same vendor works well together; and also offers better security through vendor-specific software configurations and security features. In order to keep this simulation as constructively generic as possible, the selection of hardware, software and operating systems in this simulation was kept as vendor-neutral as possible.

- **Use of a wireless router that has common consumer features**

  Using features and configurations common to most consumer brands of wireless hardware and software would allow the steps discussed in this study to be easily adapted in diverse environments.

Based on the above factors, this simulation would include:

- Three laptops
- Two desktops
- One printer

The above would be networked using a wireless router. Wireless client hardware would be selected to represent common consumer brands and types.

© SANS Institute 2005 Author retains full rights.

3.1 Hardware selection

3.1.1 Wireless client adapter hardware

The variations available in wireless client adapter hardware were:

- USB-powered wireless client adapters
- PCI cards for desktops
- PCMCIA cards for laptops
- Wireless cards built into laptop motherboards
- A wireless-to-Ethernet converter

After a review of consumer trends for popular brands and types, the following were chosen for the simulation in order to closely approximate both the authorized user volume and the occasional guest user with "non-standard" hardware:

  - D-Link USB (DWL-120) connected to a Pentium-4 desktop running Windows XP Home edition
  - Cisco 350 connected to a Pentium-3 laptop running Windows 2000 Professional
  - Dell TrueMobile connected to a Pentium-4 M running Windows XP Professional edition
  - An Intel Centrino-powered Pentium-4 laptop with wireless connectivity built into the motherboard
  - A video game console connected to a D-Link Wireless-to-Ethernet converter (DWL-810+)

The steps detailed through this study are designed to have a minimal effect on the type of client machine / hardware and are not intended to be specific to the operating system, thereby offering support for guest users with non-standard wireless networking hardware and software

3.1.2 The wireless router

- **Wireless router: D-Link DI-614+**

  D-Link is popular consumer brand for computer accessories, consumer electronics and a reputed name in wireless routers and wireless client adapters (USB, PCI and PCMCIA cards). Furthermore, after reading through a few manuals at the D-Link site, I found that the configuration screens and most of the security features of their routers were close counterparts of each other and to other brands as well. Therefore, the features and settings discussed in this paper for this specific router could easily be applied to higher revisions for similar results.

© SANS Institute 2005 Author retains full rights.

4 Access control

Access controls based on roles and rules are critical to any multi-user network environment that allows access to sensitive data and resources. Such controls are intended to restrict access based on the concept of 'least privilege', i.e. access to data and resources is limited strictly to the scope of the user's business function.

However, in the average home office wireless network environment, users associate themselves with a single domain; i.e. the wireless router that performs the dual task of facilitating the wireless connectivity and networking the users. Therefore, configurations available on the router towards access control cannot be easily implemented with the granularity of user-based restrictions to specific data repository and resources. These features are often deployed in larger-scale commercial and wide-area wireless networks wherein the expected user volume is high and the subsequent risk from malicious users is also significantly high.

For the home office environment, access control can be limited in a rudimentary "authorized users" and "unauthorized users" manner, with the simple and singular distinction that only authorized users can access all the resources on the network. For increased security, these network resources could be configured to leverage independent authentication systems, i.e. a networked computer or print server enforcing Windows authentication.

In the context of securing the wireless network, the concept of access control can be loosely described as:

- **Customized configurations**
  Non-standard configurations that thwart most common attacks

- **Authentication**
  Being able to recognize an authorized user of the wireless network

- **Logging**
  Monitoring and logging user access

- **Physical security**
  Restricting the wireless coverage area within the desired physical space

- **Automated intrusion detection**
  Using an automated means of verifying the integrity of the network

© SANS Institute 2005 Author retains full rights.

4.1 Customized configurations

As an increasing number of network audit tools get posted on the Internet, there are a higher number of "script kiddies" [3], i.e. people with a fairly low amount of talent in the network arena whose intent in using such tools is the quick and easy compromise of a targeted network or system.

Most of these tools are developed so that their default settings are fairly generic, and are intended to be effective on a network with most of the vendor default settings left in place by the network administrator. While these tools do offer modes and means of customization so that they can be used on non-standard networks as well, it requires a fair amount of network-related knowledge and expertise to execute such customizations.

Thus, changing the vendor's default settings to a customized value is often the first line of defense against common, "script kiddie" attacks on any network setup. In addition to offering a modicum of security, changing vendor defaults to customized values often helps in making network setups user-friendly. For example; authorized users of the wireless network would identify a known "name" for the wireless network a lot easier than the vendor default alphanumeric value.

Within the home office wireless network that forms our testbed environment for this study, the following measures can be taken towards changing the vendor's default settings on the wireless router:

- **Changing the default identification of the network**

  By default, most wireless routers are given an alphanumeric value as their "name" i.e. an alphanumeric value for the radio beacon that the wireless client adapter can detect when it scans the wireless spectrum in its proximity. Users can see such "names" in their wireless client software, and choose to associate with any one at any given time.

  Over time and increased percolation into the consumer market, it has become commonplace to find the vendor default "names" for consumer wireless router left in place by their users. Since each vendor follows a specific nomenclature, the practice of sticking with the vendor default "name" for the wireless network allows malicious intruders to easily identify the brand of the wireless router being used. With this knowledge, the attacker could tailor the attack routines by using known vulnerabilities and exploits specific to that brand.

[3] See Script Kiddie.

© SANS Institute 2005 Author retains full rights.

Changing the "name" of the wireless network, also known as the wireless network's SSID (Service Set Identifier) allows for a moderate measure of security against this type of threat. An increasing number of publicly-available wireless audit tools now have the capability to identify the vendor / brand of wireless hardware being used by a network irrespective of whether the SSID is changed by the user or not. However, this still is a recommended first step towards securing your wireless network.

- **Hiding the SSID**

Building on the previous step, most wireless routers also offer a feature whereby the broadcasted network name, i.e. the wireless network's "SSID", is hidden.

This feature has its advantages and its disadvantages. The primary advantage is that only the users who know of the network and its SSID, would be able to configure their wireless network client adapters to look for the hidden SSID, thereby building another layer of security against the malicious intruder.

4.1.1 The Wireless Zero Service in Windows XP

The Wireless Zero Service configuration in Windows XP is one of the main deterrents against this premise. Windows XP ships with a default service, called the "Wireless Zero Service" configuration that lets the operating system detect the strongest wireless signal in its proximity. Following identification of such a signal, the operating system attempts to associate with it in order to provide the user with the best wireless connectivity.

When the "SSID hiding" feature is enabled on a wireless router, Windows XP often has trouble staying associated with the hidden SSID. This leads to frequent connection drops because the operating system translates the hidden SSID as an unavailable SSID and tries to find and associate itself with a stronger signal.

In addition, the Windows XP Wireless Zero Service is configured such that it does not require user intervention when switching to a different wireless network – unless the new network enforces user authentication in the form of an access token like a WEP key. Furthermore, this service also has to be specifically configured to differentiate between peer-to-peer wireless connectivity and wireless connectivity provided by an access point / wireless router.

© SANS Institute 2005 Author retains full rights.

Since the signal strength of an average peer-to-peer radio beacon is often much stronger owing to proximity than that of a wireless router, Windows XP users often find their wireless connection transparently switching to a different wireless network, or to a peer-to-peer network.

The Wireless Zero Service configuration in Windows XP is enabled automatically at system startup, but can be turned off by the user if so desired. This requires command-line execution [Start > Run] of the following commands:

- "net start wzcsvc" (without the quotes) - to start the service and have Windows XP automatically locate the wireless networks in the area, and attempt connection to the strongest one
- "net stop wzcwvc" (without the quotes) – to stop the service and use the wireless network client adapter software to locate the wireless network of choice and connect to it.

Furthermore, several public distribution wireless network audit tools have now been developed with features that allow them to detect hidden SSIDs as well.

Hidden SSIDs are often a subject of debate [4] when it comes to their merit as a valid security safeguard for a wireless network. Given the prevalence of Windows XP and its default activation of the Wireless Zero Service configuration, I would advise against enabling this feature while configuring the wireless router.

- **Changing the default network location of the wireless router**

By default, most wireless routers assign themselves the internal network location of 192.168.0.1. At this location, the router hosts a Web application that allows access to the wireless router's administrator console, which controls all the access and security controls implemented on the network.

Changing the wireless router's default IP address on the internal network makes it a tad more difficult for an intruder who has gained access to the network, to access the administrator console.

The administrator console also enforces user authentication via a username and password.

[4] See Moskowitz.

© SANS Institute 2005 Author retains full rights.

- **Setting a complex administrator password**

  A complex administrator password on the wireless router is critical to the security of the wireless network. If an attacker has managed to penetrate the network, the administrator console could be one of the first targets since it would allow the attacker to disable any other security / logging features.

  If the attacker cannot guess the password, a commonly-used approach is to use a brute-force password-guessing tool that uses a continually increasing permutation of alphanumeric values till it reaches the right password. A complex password makes it harder for both the attacker and a brute-force password-guessing tool to gain authenticated access the administrator console. A combination of two or more of the following criteria would help towards selecting a sufficiently complex password:
  - The length of the password should exceed 8 characters
  - The password should have a combination of lowercase and uppercase characters
  - The password should not directly use any socially-available data about you, i.e. your name, birth date, family members' names, pets' names, car license plate, etc. A combination of these values could be used.
  - The password should contain special characters, i.e. the period symbol, the ampersand symbol, etc.

- **Enabling the in-built firewall**

  Most wireless routers today have a "firewall" feature that helps protect the network from a significant volume of known threats. Vendors usually publish free updates and patches that revise such firewall functionality on wireless routers.

- **Disabling any default server implementations**

  Some routers have default server implementations that could be enabled out of the box. All of these should be disabled and then enabled on a case-by-case basis based on business / personal needs. Ideally, even when such functionality is required, it should be enabled only for the duration for which it is required, and turned off immediately after.

- **Disabling any default internal network access granted by the router**

  Although rare today, some routers ship with a default vendor setting that allows access to a certain internal IP address. The vendor's intent in doing so could be letting consumers easily make content available to the Internet in the form of Web pages, pictures, etc. Such features should be enabled on a case-by-case basis, only for the duration for which they are required.

© SANS Institute 2005 Author retains full rights.

- **Enabling restrictive DHCP leasing**

  Wireless routers connect several users wirelessly. For these users to associate themselves to the network, the wireless router has a Dynamic Host Control Protocol (DHCP) server whose function is to assign an IP address to every new computer that joins the network.

  These IP addresses are given out as leases, i.e. an IP address is granted to a user on the network only for certain duration of time, known as a "DHCP lease". Once this "lease" expires, the IP address can be re-used for another user if the previous recipient is no longer associated to the network.

  Most wireless routers have a feature that lets users specify how many such leases can be granted by the router. Restricting this number to the number of expected authorized users and a reasonably small number of guests makes for a good security control.

  For example, in the home office environment that is discussed in this paper, the expected volume of authorized users is around five. Thus, the DHCP configuration should be altered such that only five DHCP leases can be granted by the router. This way, under average working conditions, the entire expected user volume will have a DHCP lease and will be able to operate normally. In the even that an authorized guest attempts to associate to the wireless network, the system administrator would have to enable the additional DHCP lease for him / her after adding his / her MAC address to the MAC address filter list on the router.

  If an attacker were to try gaining unauthorized access by faking an authorized MAC address, the router would restrict the attacker's attempt to associate with the wireless network because there wouldn't be an available DHCP lease to grant to the attacker's computer.

  In this event, the attacker would have to wait until an authorized user went offline. However, the DHCP lease duration can be set to its maximum value, which is usually one week, so that the length of time that the attacker has to wait till the DHCP lease is available for his / her use is fairly high – thereby mitigating the attack.

© SANS Institute 2005 Author retains full rights.

4.2 Authentication

4.2.1 Two-factor authentication

The concept of two-factor authentication is often summarized anecdotally as: "Something you are and something you have". Translated, authentication based on a characteristic of the user that the system being accessed recognizes, combined with an access token of some sort that this user provides the system as an entry key.

In the context of the subject at hand, without requiring the deployment of any additional authentication-related software, we could use the following towards two-factor authentication:

- **A client machine's MAC address**

The MAC address is a tangible identification parameter that is a fundamental requirement for any networked computer. Since this is intrinsic to the user's network hardware and a value that the user cannot easily change, it can be easily leveraged as one of the two halves of a two-factor authentication sequence. Most wireless routers today have the ability to allow access only to a certain set of MAC addresses. In the next section, this paper will describe the configuration necessary to implement 'MAC address filtering' on the wireless router used.

- **The WEP / WPA key as an access token**

WEP is an acronym for Wired Equivalent Privacy, a protocol that is used to secure access to a wireless network. Over the years that wireless networking technology has climbed towards its current position in the consumer marketplace, various experts have spent considerable effort detailing the weaknesses of this protocol as a sufficient security safeguard for a wireless network.

Recent revisions of wireless networking protocols have led to the incorporation of this feedback into a stronger security protocol called Wi-Fi Protected Access [5], abbreviated "WPA". Older wireless networking hardware, especially routers using 802.11b; do not usually have native support for WPA. However, most hardware vendors have recognized this development and have issued the requisite software / firmware patches via their support websites.

[5] See W-Fi Protected Access.

© SANS Institute 2005 Author retains full rights.

From the perspective of two-factor authentication, a WEP / WPA key could act as an access token; granted by the system administrator to an authorized user for access to the wireless network.

Thus, for a user to access the wireless network, one would need:

1. A machine whose MAC address is included in the router's MAC address filter
2. The correct WEP key for that network

In addition to facilitating verifiable authentication, the reliance of a computer on its MAC address while connected to a network can also be leveraged to effect automated intrusion detection. This aspect is detailed later within this section.

4.3 Logging

Based on my research with different consumer brands of wireless router hardware, the logging functionality is fairly comprehensive and easily accessible via the administrator interface.

Common log elements include:

- Timestamp of event recorded
- Network events, i.e. DHCP leases being granted to new computers associating with the network, broadband connection status, etc.

4.4 Physical security

By definition, the wireless network is one that exists without the conventional physical boundaries of cabling ducts in walls and network cable for connections.

This makes way for portability**,** one of the most significant advantages of a wireless network. However, as with most things, the best asset can often be the worst liability. The extended accessibility on offer thanks to a wireless network can pave the way for malicious attackers, especially when high-powered antenna arrays and similar hardware can be trained on wireless networks in order to gain access from a distance.

In addition, it has become increasingly simple to find tutorials on the public Internet that offer detailed steps to build wireless antennae from common, low-priced household items. Thus, it is very important to limit and/or restrict the area covered by a wireless network; i.e. the area within which anyone can attempt to

© SANS Institute 2005 Author retains full rights.

connect to your wireless network. Given the intangible nature of wireless signal coverage, an effort to contain it is often viewed as fundamentally unsound. Nevertheless, there are certain precautions that one can take to limit physical access to an area covered by a wireless network. These include the use of signal attenuators to contain the wireless network signal coverage within the intended physical perimeter and the use of a directional antenna to employ a focused coverage beam pattern within the intended physical perimeter.

4.5 Automated intrusion detection

An automated, always-on means of detecting the presence of an intruder completes the creation of this security system. As mentioned earlier, the wireless router's "MAC address filter" can be used as a means of facilitating client authentication to the network. Leveraging this concept further, a "MAC address filter" can also be used to continuously monitor the network for MAC addresses that are not a part of the router's MAC address filter list; and to generate alerts if such an event were to be detected. Ideally, such an intrusion detection system should have the following features:

- **Always-on operation**

  This would ensure that the intrusion detection system and the wireless network are always working in concert.

- **Be deployed on a system separate from the router**

  The administrator console on the average consumer wireless router is protected by a single username and password. In the event that an attacker were to guess the right password or launch a brute-force attack to obtain the password to the administrator console, it would be very easy to turn off all the security safeguards on offer via the router's configuration. Therefore, in an effort to implement a scheme of checks-and-balances towards the security of this environment, the intrusion detection system should be deployed on a separate computer.

- **Able to quickly identify all the users and traffic on the network**

  One of the main goals of implementing an automated intrusion detection system is to be notified immediately after any unauthorized user / traffic activity is detected on the network. Thus, such a system should be able to recognize new users and changes to traffic activity quickly, and be in a position to generate automated alert notifications immediately upon detection. I

© SANS Institute 2005 Author retains full rights.

The concept of a "demilitarized zone" is often discussed in tandem with intrusion detection. The wireless router chosen in this study does have the feature of implementing a demilitarized zone" i.e. having one computer intentionally made available to the Internet to serve as a machine that can be scrutinized by the system administrator for unauthorized access attempts.

4.5.1 AirSnare

Evolution in the realm of technologies in the domain of (automated) intrusion detection has led to several refinements over the years. Most intrusion detection systems today check for "attack signatures" i.e. a known attack vector value or behavioral pattern that allows the system to understand the type of attack it is being subjected to. Following such identification, automated controls and scripts are often initiated towards deploying alert notifications, forensic logging and security countermeasures.

Intrusion detection in the domain of wireless networking has also seen similar significant improvements. There are technologies available today that allow rogue access points and unauthorized clients to be identified by an approximate geographical marker using their incident signal strength and a global positioning system. Current examples of countermeasures include the utilization of a controlled denial-of-service attack on such rogue access points so that they are rendered ineffective if found within an area where such access points are deemed unauthorized by the applicable security policy.

The automated intrusion detection system described in this study is an effective means of checks-and-balances on the security measures implemented by the router. Called "AirSnare" [6], it is available as a free download off the Internet. Contrasting its feature set against that of recent commercial intrusion detection software, its functionality that may seem fairly primitive. However, it performs the critical tasks of:

1. Continuously monitoring the network for the presence of any previously-unknown MAC addresses
2. Notifying the system administrator when a previously-unknown MAC address is detected on the network, via audio / visual interface cues and via email
3. Allowing the system administrator to notify intruders of their unauthorized actions

---

[6] See AirSnare.

© SANS Institute 2005 Author retains full rights.

Aside from being freeware, AirSnare has various advantages for the home office environment:

- It does not necessitate that a computer be dedicated to the sole task of automated intrusion detection. The computer on which AirSnare is running can be used for other network / computing tasks as usual.
- The AirSnare application does not impose unreasonably high system or network requirements for successful deployment
- The interface and controls are fairly intuitive and require a minimal level of user training
- The logs and alarms generated by this application are user-friendly and offer a concise-yet-comprehensive description of the network activity being monitored
- Its operation is completely passive and does not adversely effect the operation or performance of the network in any way
- It identifies all the active network computers quickly. If a potential intruder is identified on the network, it has a feature that allows the system administrator to notify this potential intruder via an alert pop-up dialog box containing customizable text.
- It offers a fair amount of granularity over its monitoring capabilities. Advanced users can opt to monitor all / either of traffic related to MAC address, TCP activity or UDP activity.
- Results can be viewed within the application interface and/or using Ethereal, another common network-log parsing tool
- It allows the system administrator / application user to monitor the specific network activities of any MAC address detected by it

Note: AirSnare should be deployed from a computer that associates solely with the wireless router. Its operation can be hindered if it is used on a computer that associates with another network, i.e. if that computer is used to connect to another network via VPN.

Given the above characteristics, AirSnare was a good fit for the environment being discussed in this paper. Its operation will be described along with the other security steps detailed in the next section.

© SANS Institute 2005 Author retains full rights.

5 Securing the network

Let's recap the security precautions detailed in the previous section.

Customized configurations

- Changing the SSID
- Cloaking the SSID
- Restrictive DHCP leasing
- Changing the default network location of the wireless router
- Enabling the in-built firewall
- Disabling any default server implementations
- Disabling any default access granted by the router to any internal network address

Authentication

Using WEP / WPA keys and a MAC address filter

Logging

Using the wireless router's logging function for a real-time view of users associated to the network. System administrators should check the logs periodically to ensure that only authorized users are using the network

Physical security

Using some means of limiting and/or restricting physical access to the wireless network's coverage area to the intended user community

Automated intrusion detection

Using an AirSnare deployment on a separate computer within the network to serve an automated intrusion detection system

© SANS Institute 2005 Author retains full rights.

5.1 Customized configurations

The following screenshots will show how to:

1. Change the default SSID of the wireless router

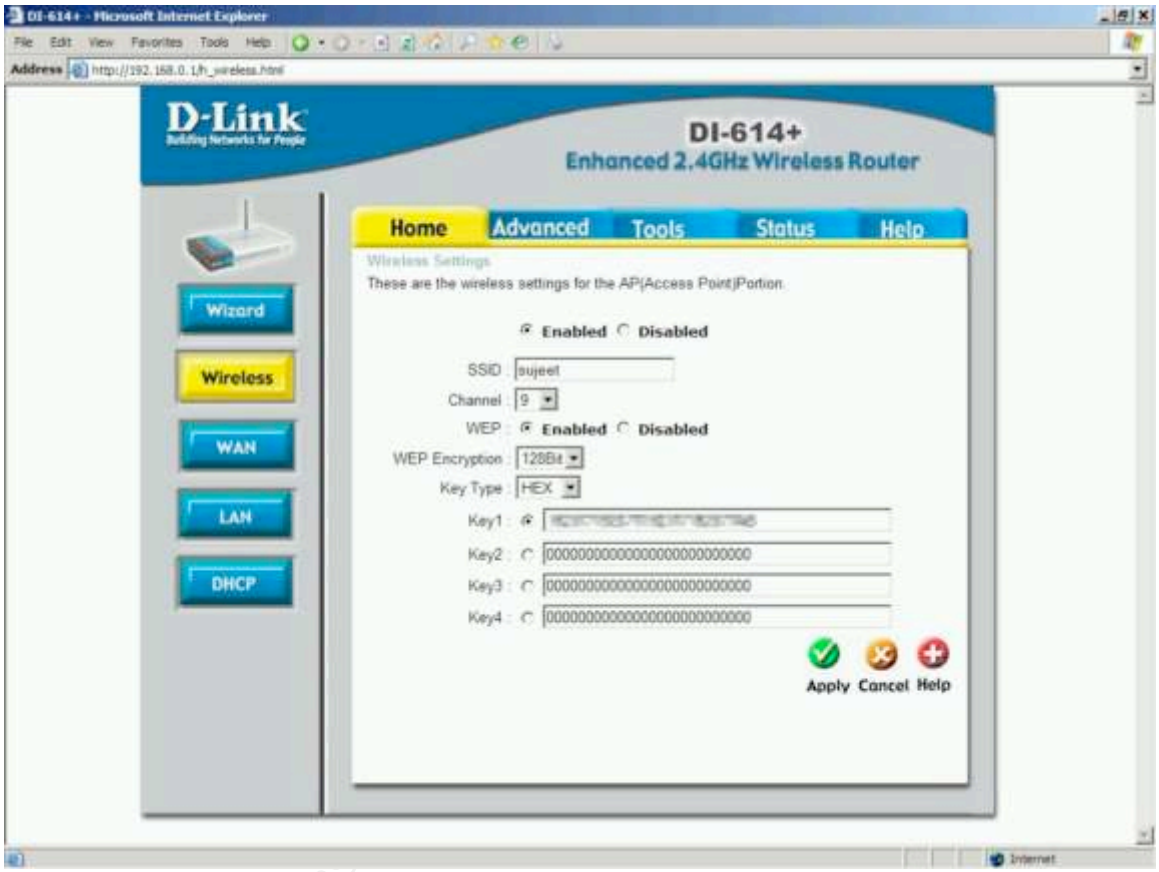


Figure 1: The administrator console showing the SSID-change screen

The above screenshot shows the configuration screen of the DI-614+ that lets the user change the SSID, i.e. the name of the network, to any value. In this example, the SSID has been changed to 'sujeet'.

© SANS Institute 2005 Author retains full rights.

2. Change the default network location of the wireless router

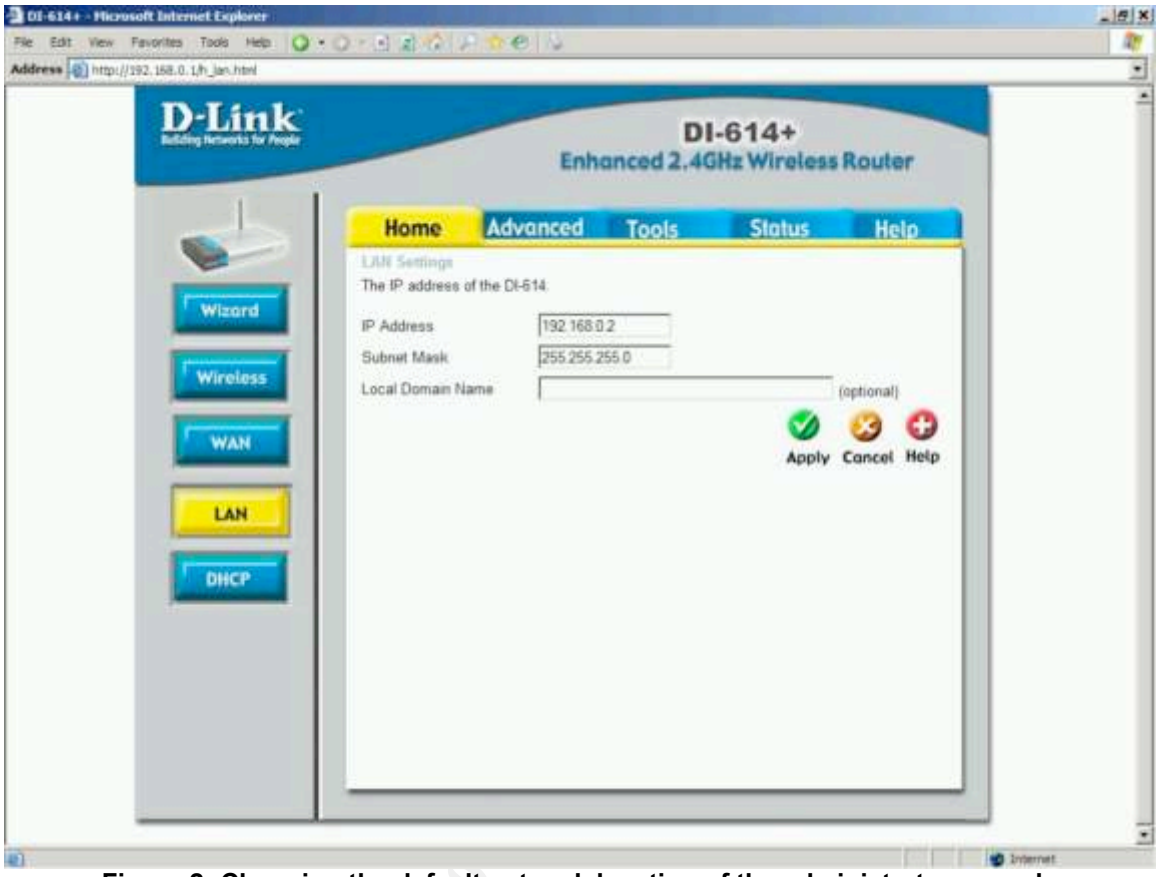


Figure 2: Changing the default network location of the administrator console

The above screenshot shows the configuration screen of the DI-614+ that lets the user change the default network location of the router. In this example, the default location has been changed from the vendor-defined setting of 192.168.0.1 to 192.168.0.2

This will change the location of the Web server hosting the administrator console Web application.

© SANS Institute 2005 Author retains full rights.

3. Enable the in-built firewall functionality

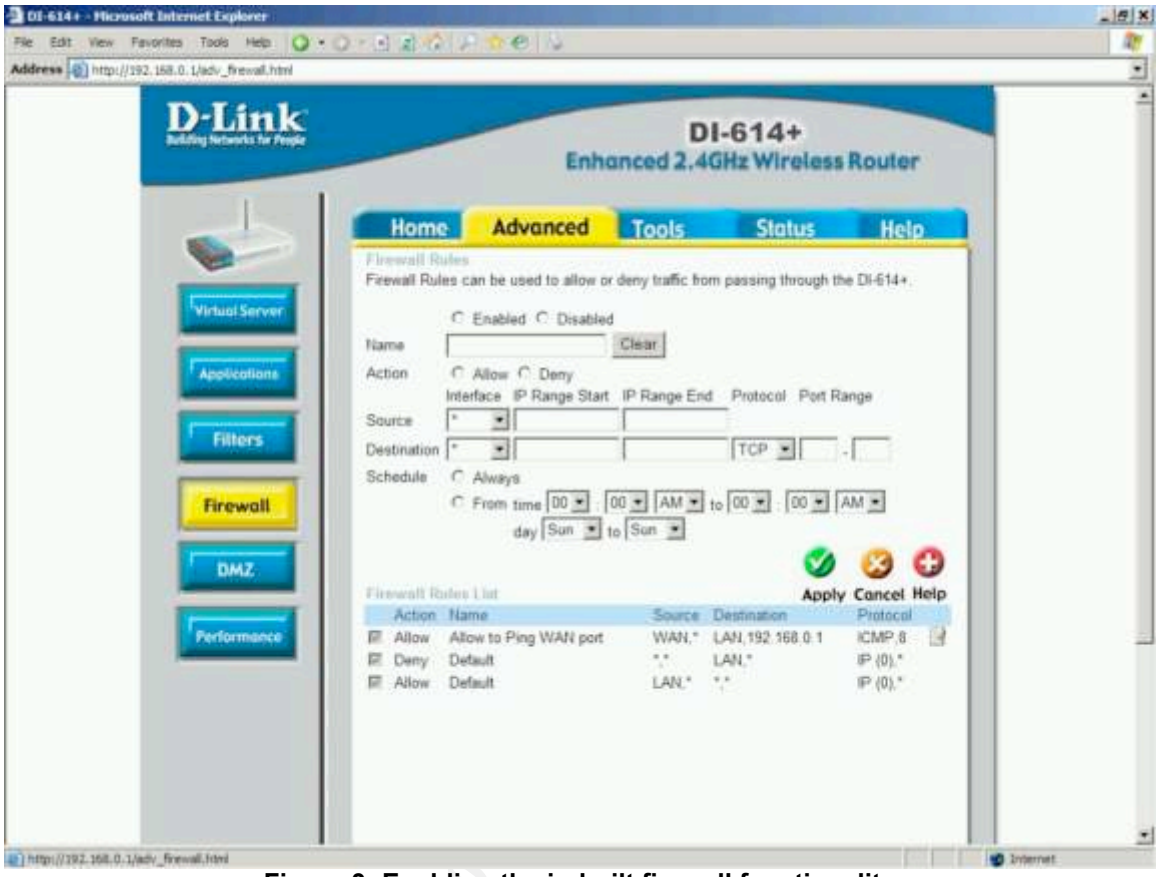


Figure 3: Enabling the in-built firewall functionality

The above screenshot shows the DI-614+ configuration screen that allows the user to enable the in-built firewall functionality. The rules checked under the "Firewall Rules List" section show that the firewall blocks any traffic from an undefined source address into the internal network and any traffic from the internal traffic to an undefined destination address. In addition, it also blocks any pings from the router to itself; since that cannot be a valid network event. The user can create additional rules based on specific needs.

© SANS Institute 2005 Author retains full rights.

4. Disable any default server implementations



Figure 4: Disabling unnecessary server access

The above screenshot shows the configuration screen for the DI-614+ that allows the user to enable and disable specific protocol and IP-related access for specific server implementation. The router comes with a list of common server implementations, but the user should ensure that only those needed by the environment are turned on. In this example, all of them were turned off.

© SANS Institute 2005 Author retains full rights.

5. Disable any default externally-accessible internal network location

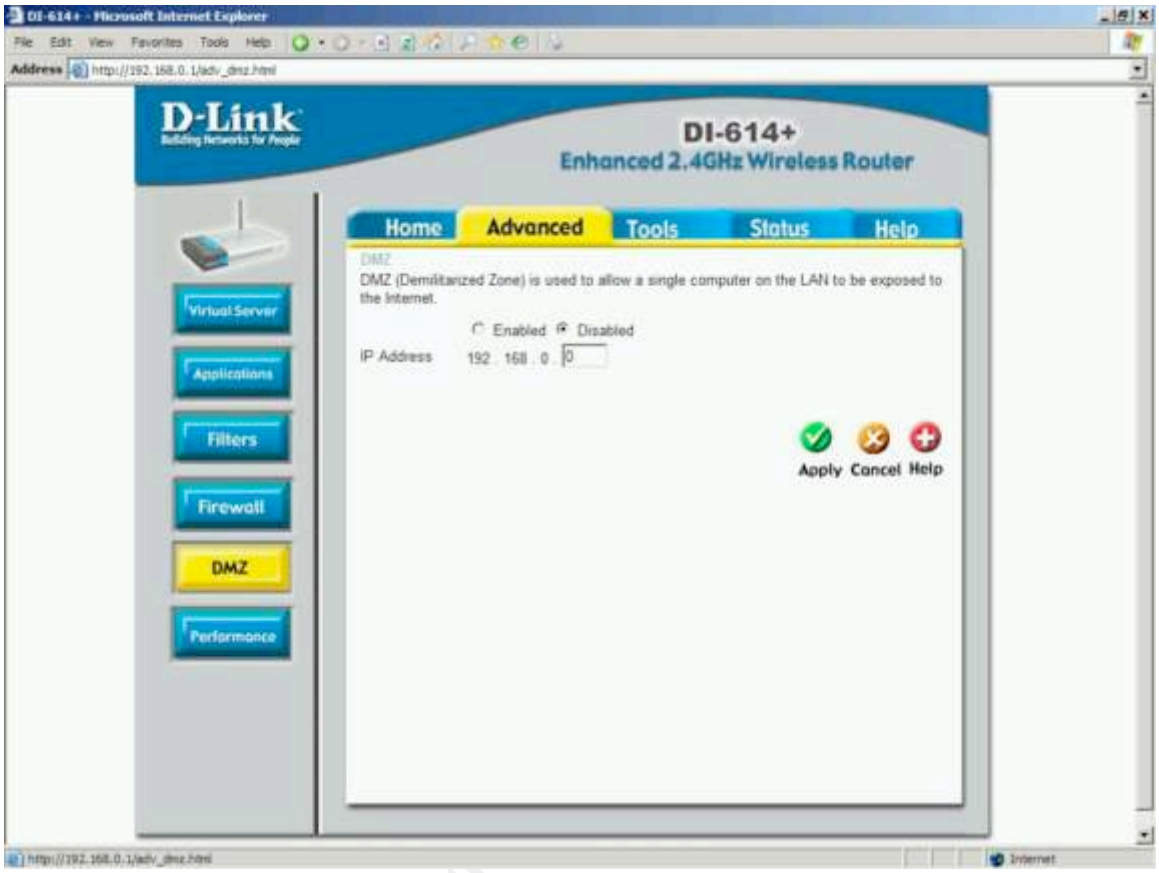


Figure 5: Disabling the DMZ

As mentioned in the previous section, a “demilitarized zone” (DMZ) can be implemented on the network by making one computer / network location accessible to the public Internet. There are various uses for such a feature, but this feature was turned off in this study. By default, this feature is turned off and should be kept that way unless there is a specific need to enable it.

© SANS Institute 2005 Author retains full rights.

6. Enable restrictive DHCP leasing

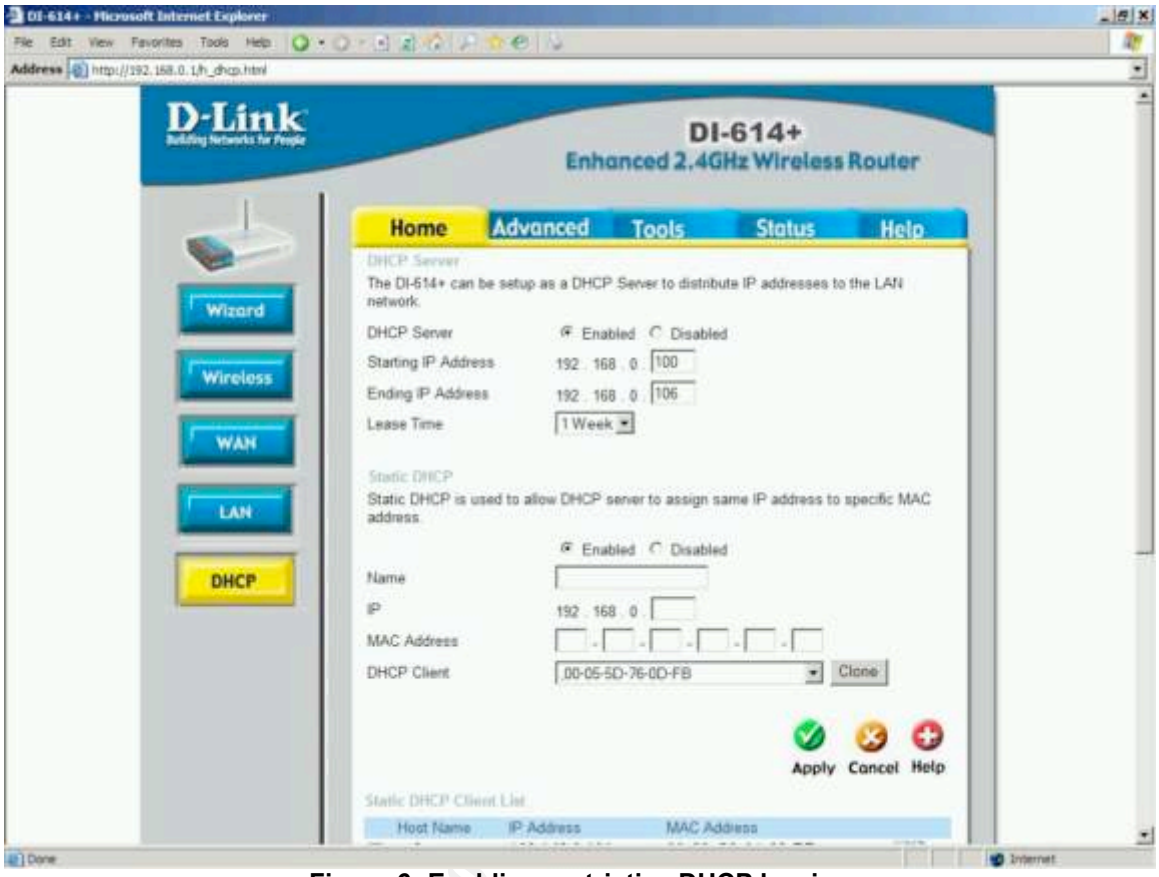


Figure 6: Enabling restrictive DHCP leasing

As mentioned earlier, this environment was designed to simulate a home office environment with five computers. The DHCP lease has been configured to allow only seven computers to access the network.

The MAC address filter shown in the following section shows that seven MAC addresses are allowed access to the network. Thus, the DHCP lease has been reconfigured such that it can allow the maximum amount of expected users to access this network.

If all these users were to be accessing the network at the same time, and a guest user were to request access; the system administrator would have to increase the DHCP lease by one, i.e. from 192.168.0.106 to 192.168.0.107. In addition, the guest user's MAC address have to added to the MAC address filter and the guest user would have to be given the WEP key in order to access the network.

© SANS Institute 2005 Author retains full rights.

5.2 Authentication

The following screenshots will show how to:

1. Enable WEP and choose a HEX key value because ASCII key values are known to be relatively insecure

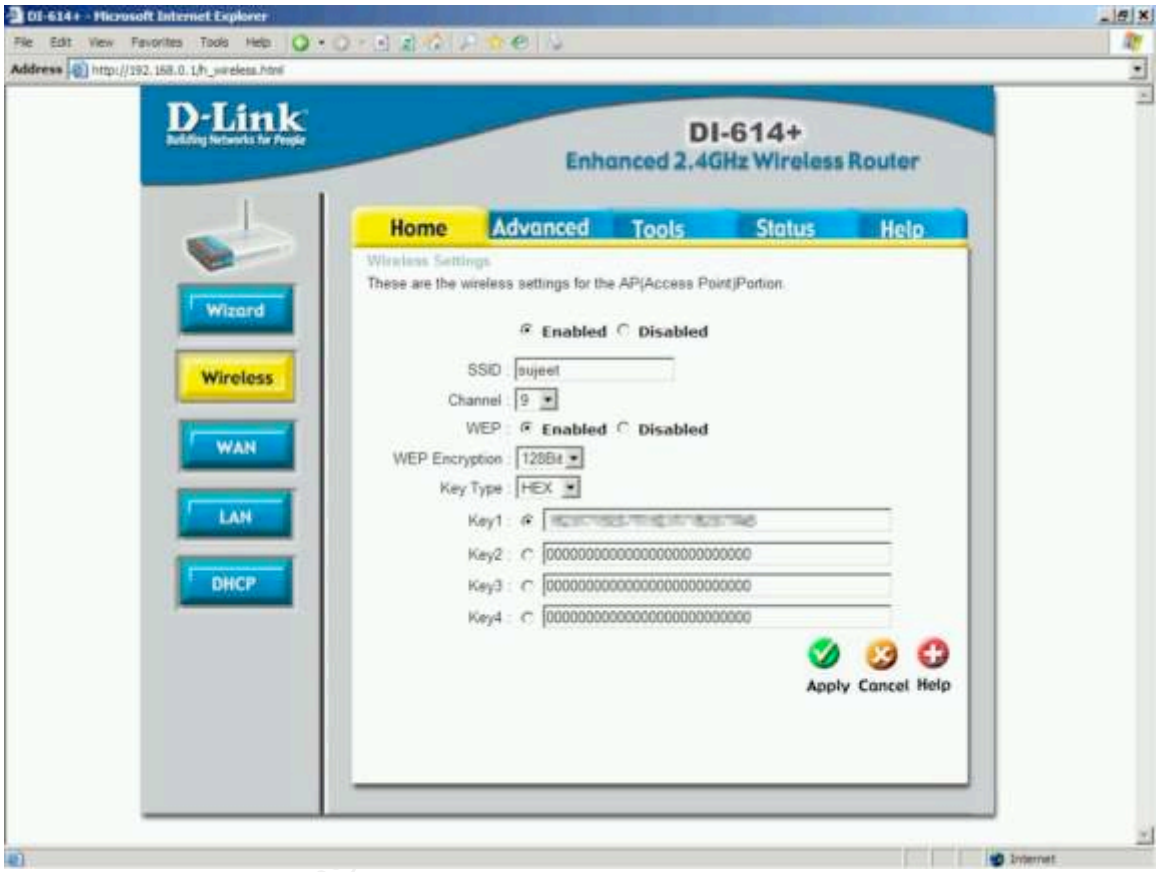


Figure 7: Enabling WEP and using a HEX key

My research of tools available to compromise the security of a WEP key (AirSnort [7], WEPCrack [8]) indicated that they were most effective on WEP keys that had an ASCII value.

Users often choose an ASCII value because it can be a user-friendly alphanumeric value, akin to a password, that can be easily remembered. HEX values, on the other hand, are harder to remember because one can select between a fairly restrictive set of numbers and alphabets; and also because one has to generate a password that is 26 characters long.

[7] See AirSnort.
[8] See WEPCrack.

© SANS Institute 2005 Author retains full rights.

2. Enable MAC address filtering



Figure 8: The MAC address filter

The above screenshot shows the configuration screen of the D-Link DI-614+ that deals with enabling filters. The D-Link DI-614+ allows the user a choice of four filters, i.e. the administrator can implement an IP filter to restrict users accessing a certain internal or external IP address and/or restrict access to certain URLs and/or to certain domains and/or by using the client MAC addresses.

Each filter exists in a disable / allow / deny state; i.e. it allows the administrator to disable the filter, or configure it such that it will allow access only when the user entry values matches the values indicated in the filter, or such that it denies access when the user entry values match the values indicated in the filter.

The MAC filter is shown in the above example. It is enabled, and configured such that only the MAC addresses indicated in the list shown are allowed access to the network. Thus, access is restricted to computers having MAC addresses belonging to the list; i.e. computers authorized for access to the network.

© SANS Institute 2005 Author retains full rights.

5.3 Logging

The following screenshots will show how to:

1. View the log window and configure the logging feature to capture maximum details about network events
2. Understand network event details from the log data captured

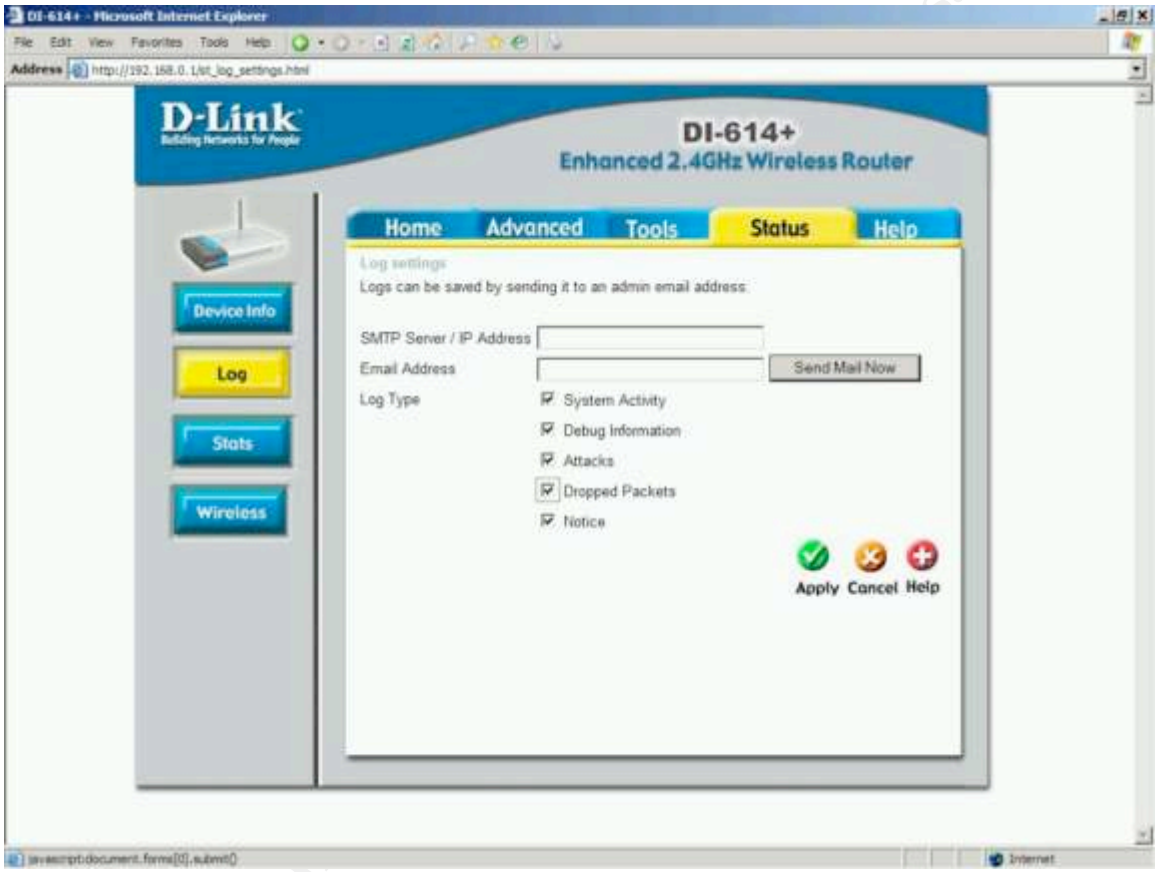


Figure 9: Configuring the logging feature of the router

The above screenshot shows the configuration screen in the D-Link DI-614+ administrator console that deals with log settings. As seen above, the router allows system activity, debug information, attacks, dropped packets and any notifications to be logged and displayed via the log viewer.

It also allows these logs to be sent via email. This could be a very handy feature if the system administrator wanted to be automatically notified of important network events like potential attacks and dropped packets.

To do so, the system administrator would have to check only the types of log data that was to be monitored, and then enter a valid SMTP address for a mail

© SANS Institute 2005 Author retains full rights.

server that would process the automated email notification process, and finally – and email address where the administrator could receive these alerts.



Figure 10: Examples and analysis of log data

The above screenshot shows the log viewer screen from the D-Link DI-614+ administrator console. The router logs 20 pages of log data. The logged data can be analyzed in the following manner:

Time: "Apr 05/2005 21:05:44" – The timestamp for the recorded network event. The router has two features that allow for accurate timing of network events; via a network time server and via a manual configuration screen/

Message: "Wireless PC connected" – This statement shows that a successful association has been made between a wireless computer and the router.

Note: "00-…" – This is the MAC address of the wireless computer mentioned earlier.

This is corroborated by the next log event recorded by the router, in which the "Message" field shows that a DHCP lease bearing a certain IP address was granted to a computer with the same MAC address.

© SANS Institute 2005 Author retains full rights.

The system administrator can thereby surmise that a computer named "MTVL04A200880" associated wirelessly with the router. This computer was granted an IP address of 192.168.0.104 and had a MAC address that matched one of the MAC addresses on the MAC address filter list [9].

5.4 Physical security

The following section will describe the use of a directional antenna versus the vendor-default and commonly-used omni-directional antenna

Wireless routers ship with an omni-directional antenna. This kind of antenna has a coverage pattern similar to the illustration below, i.e. it extends its zone of wireless connectivity in the shape of a sphere around itself.

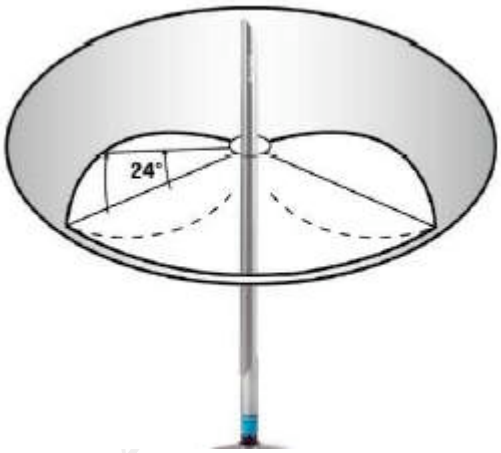
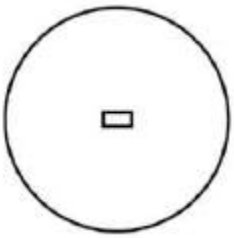
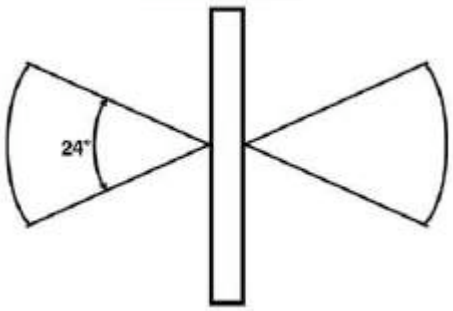


Figure 11: Views of an omnidirectional antenna's signal coverage pattern [Diagrams taken from the documentation for the D-Link ANT24-0700 Omni-Directional 7dBi Indoor Antenna; ftp://ftp10.dlink.com/pdfs/products/ANT24-0700/ANT24-0700_ds.pdf]



Horizontal view



Vertical view

A coverage pattern of this nature can extend outside the physical perimeter of the home office environment quite easily, especially if the router is placed in an inconspicuous corner or similar area.

[9] The MAC address filter, Page 25.

© SANS Institute 2005 Author retains full rights.

One of the following methods can be adopted in order to contain the signal coverage of the wireless router's antenna within the physical perimeter of the home office environment:

- Using signal attenuators to degrade the wireless network radio signal as it passes past the physical perimeter

  This solution could theoretically satisfy all the aspects of this problem, but could potentially need several signal attenuator pads to adequately contain the radio signal within the intended physical space.

- Using a directional antenna

  The coverage pattern of a directional antenna is in the form of a somewhat conical beam, as indicated by the illustration below. An antenna with such a coverage pattern can be easily positioned in a corner of the physical facility so that the coverage beam pattern covers the entire intended physical area. As long as the coverage pattern does not extend in a sphere-like fashion outside the physical perimeter, it would be harder for potential intruders to eavesdrop on the signal and attempt attacks on the network.

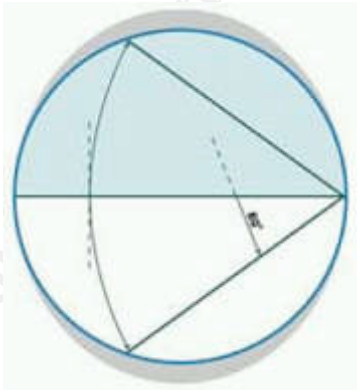
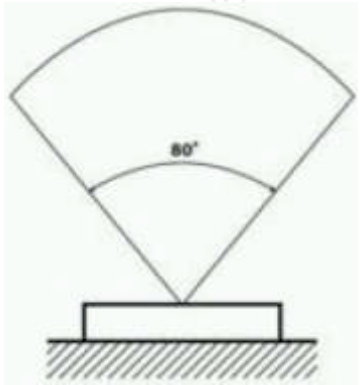
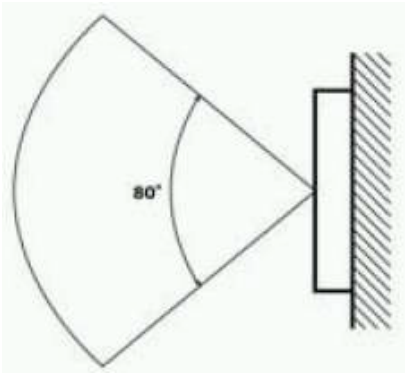


Figure 12: Views of a directional antenna's signal coverage pattern [Diagrams taken from the documentation for the D-Link DWL- M60AT 2.4 GHz Directional Indoor Antenna; ftp://ftp10.dlink.com/pdfs/products/DWL-M60AT/DWL-M60AT_ds.pdf]



Horizontal view



Vertical view

© SANS Institute 2005 Author retains full rights.

5.5 Automated intrusion detection

The following section will show an AirSnare implementation on one of the computers of the network, and its use towards:

1. Accurately identifying all the computers on the network

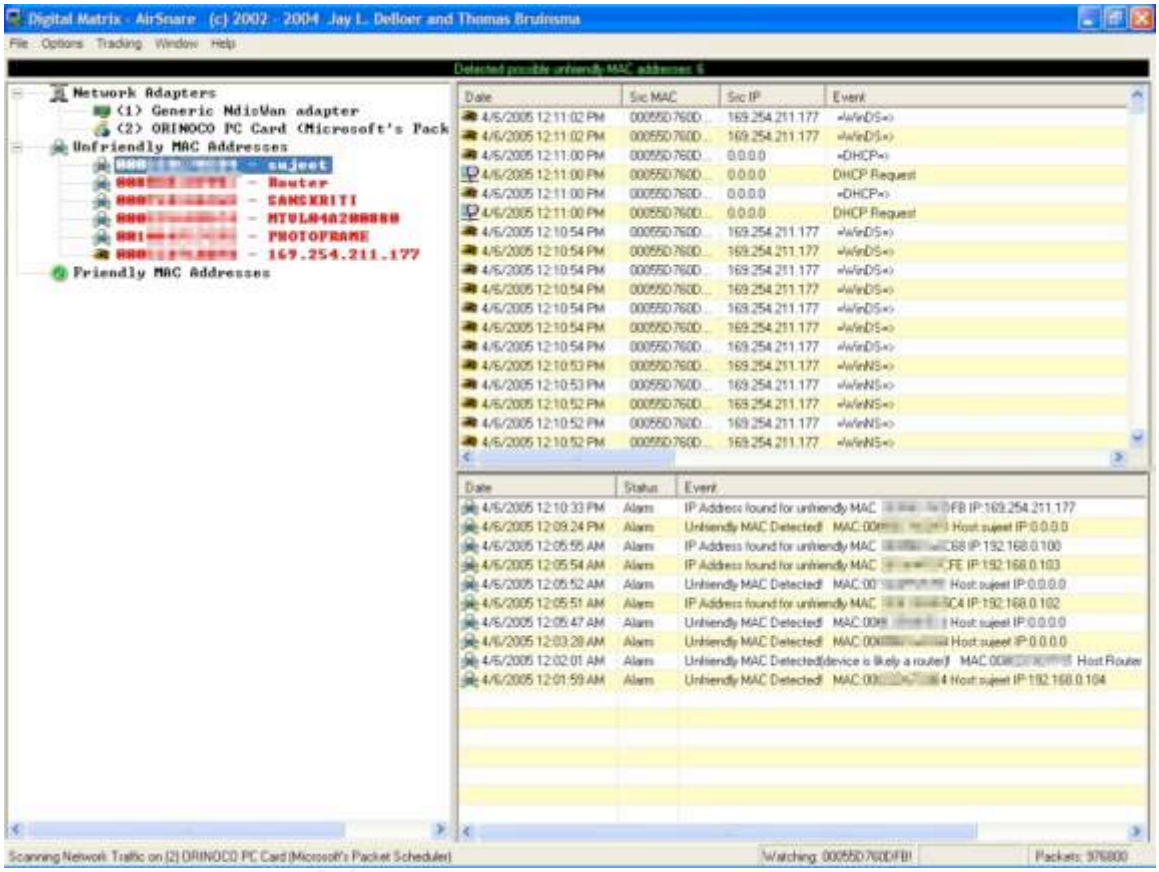


Figure 13: AirSnare interface

The above screenshot of an AirSnare deployment shows that it has identified all the active computers on the network. Since none of these were added into the "Friendly MAC addresses" list for the purpose of this demonstration, they show up as "Unfriendly MAC addresses".

2. Quickly recognizing new MAC addresses on the network

Via the above screenshot, one can also see that AirSnare has resolved the computer names corresponding to the MAC addresses and recorded the specific network events that state when an IP address was granted, etc. This data can be of immense use to the system administrator from a security perspective.

© SANS Institute 2005 Author retains full rights.

3. Troubleshooting connectivity problems by new users

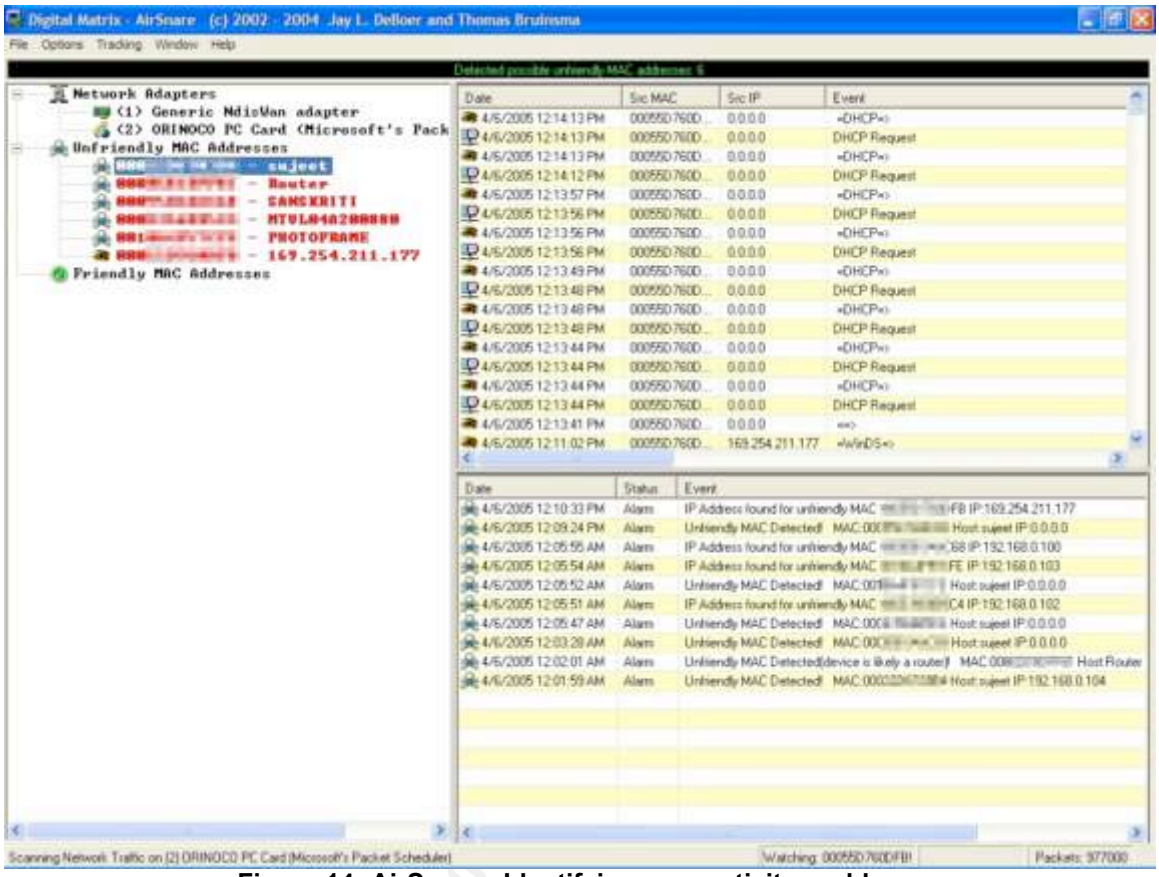


Figure 14: AirSnare - Identifying connectivity problems

For the purpose of this demonstration, one of the computers on this network was not given the right WEP key to access the network; to simulate a condition in which an intruder / unauthorized guest user managed to clone an authorized user's MAC address to access the network.

The AirSnare event window shows that the IP address for the machine without the right WEP key remains at its preset value, i.e. 169.254.211.177 and that this machine issues a string of DHCP requests to the router which are not successful because the WEP key is incorrect.

This demonstration shows that one would need both the right WEP key and the right MAC address to connect to the network.

Such logs would also help the system administrator accurately diagnose connectivity problems faced by existing users or authorized guest users.

© SANS Institute 2005 Author retains full rights.

4. Alert notification for intruders

AirSnare has a feature called “AirHorn”, (illustrated below) that lets the administrator enter some warning text and send it to any IP address associated to the internal network. This lets unauthorized users know that they are being monitored by the system administrator.



Figure 15: AirSnare's "AirHorn" module

5. **Administrator notification via email**

   AirSnare allows supports the transmission of alert notifications to the administrator via email.

© SANS Institute

© SANS Institute 2005 Author retains full rights.

6 Potential attacks and countermeasures

Given the above deployment, it can be hypothesized that an attacker could attempt compromising the network in the following manner:

1. Get within a physical area offering connectivity to this wireless network. Thanks to the use of the directional antenna, this 'connectivity zone' is severely limited to the physical facility of the home office
2. Figure out the WEP / WPA key in order to attempt associating with the wireless network. An attempt to access the wireless network based solely on the right WEP / WPA key will be easily thwarted by the MAC address filter implemented on the wireless router.
3. If the attacker were to fake a MAC address that he / she knew to belong to an authorized user of the network, the restrictive DHCP leasing utilized on the router would not allow the attacker access to the network since all the DHCP leases would be taken up by authorized users of the network.
4. In order to bypass / compromise the MAC address filter list and the DHCP leasing, the attacker's computer will have to associate with the wireless network and attempt a brute-force attack on the administrator's password. If such an attempt at unauthorized access to the administrator's console were to succeed and if the intruder were to be in a position to turn off the MAC address filter and the restrictive DHCP leasing, the router would have to restart in order to initiate these changes. If the router were to restart abruptly like this, all the users connected to the network would lose connectivity for the duration of the outage, and this could serve as a warning for the system administrator and/or the users.
5. If the attacker were to attempt such an attack during off-peak hours; the automated intrusion detection system would trigger an alert notification to the system administrator based on its detection of an "unfriendly" MAC address. Since the attacker would not know which computer this intrusion detection system was deployed on, it would be difficult to find it and turn it off before it generated the alert notification

Thus, for an attacker to successfully compromise this wireless network, it can be postulated that the following would be necessary would have to:

1. Access to the physical area covered by the wireless network
2. Access to the right WEP / WPA key to access the network
3. Ability to access the administrator console to turn off the MAC address filter, or the ability to change the local MAC address to that of an authorized user of the network
4. Availability of an unused DCHP lease

© SANS Institute 2005 Author retains full rights.

6.1 Testing the security of the network

Working within the resources and time available for this project, I attempted to simulate a network security audit of the proposed security model by running a series of tests against the network.

In summary, these tests:

- Used a high-gain wireless antenna in order to eavesdrop on the wireless signal coverage area of this environment without being physically present within the beam coverage pattern of the directional antenna
- Used Kismet to gain information about the network
- Used AirSnort to attempt breaking the WEP key protection on the network

6.2 Executing the tests

6.2.1 Using AirSnort

Goal: To identify the right WEP key for the network

Various wireless security studies indicate that WEP keys can be guessed using public distribution software in a matter of hours. In order to simulate this setting, I used the latest version of AirSnort, a Linux tool designed to break WEP keys. In addition, I also removed the wireless client adapter's MAC address from the MAC address filter list so that it would adequately represent an intruder trying to gain access to this network.

Conclusion: AirSnort was unable to guess the WEP key after 3 days of continuous operation. The chosen 26-character HEX WEP key stood up to this attack.

6.2.2 Using the right WEP key but the wrong MAC address

Goal: To compromise the network with the right WEP key, but without a MAC address that is a part of the MAC address filter list on the router

What if the attacker had managed to break the WEP key after a reasonably long period of surveillance? Assuming that the WEP key was compromised, the attacker would be restricted access to the network because of the MAC address filter list. Since the attacker's MAC address was not included in the filter list, the router will not lease out a DHCP address to his / her computer and thereby deny access to the network.

Conclusion: The attacker was denied access

© SANS Institute 2005 Author retains full rights.

6.2.3 Using the right WEP key and the right MAC address

Goal: To compromise the network with the right WEP key and an authorized MAC address

Kismet is one of the tools available on the Internet that has the potential to sniff out MAC addresses as they travel unencrypted over the air. Assuming that an attacker used a similar tool to ascertain the value of a MAC address authorized for access on this network, and changed the MAC address of his wireless client hardware to match the same; he / she would then have the required access tokens to access the network, namely:

- A MAC address recognized by the wireless router as one in its filter list
- The right WEP key for access to the network

Conclusion: The attack can result in the following two possibilities;

1. If the attacker is allowed access to the network, it will contain two computers with the same MAC address – a non-standard condition that would be visible via the router's logs as well as the AirSnare logs. The AirSnare logs would show that an IP assignment was made to a MAC address that had already been granted an IP address on the network. However, AirSnare would not generate an alert (it does so only when it detects an unrecognized MAC address).

2. If the network has all its expected users connected at the time of this attack, then all the DHCP leases would be used up and the attacker would be denied access to the network.

Thus, an attacker would need a combination of the correct WEP key and an authorized MAC address in order to gain access to this wireless network when a DHCP lease was available. This condition is probable under the following conditions:

1. The attacker were to have knowledge of the correct WEP key either by an extended WEP-cracking attack, or by compromising the security of an authorizer user's wireless client software
2. In addition to the right WEP key, the attacker would have to use the right set of tools in order to get the value of a MAC address authorized for access on the network
3. The attacker would have to time the attack when a DHCP lease was available for use
4. In addition to the above, the attacker would have to employ a reasonably high-powered antenna in order to gain access to the network without being physically present within the signal coverage pattern of the directional antenna

© SANS Institute 2005 Author retains full rights.

7 Conclusion

Wireless networks are gaining ground in the consumer market segment, and trends do not indicate any projected declines in the statistic. In addition, an increasing number of computing devices are being manufactured with wireless capabilities and being sold in the consumer market. These include wireless devices that track stocks and weather reports, wireless devices that bridge the home computer network and the home theater setup, etc. Attractive advertising and competitive pricing helps drive these into consumer homes, increasing their reliance on a home wireless network. Furthermore, the numbers associated with identity theft are on the rise and have thus led to a higher need for securing personal data; and subsequently the wireless home network.

The steps detailed in this study are intended to be simple to administer and be neutral to vendors, operating systems and hardware, thereby allowing for a wider audience. In essence, they are intended to bring out the security features available in most wireless hardware available today and to let the administrator of a home office environment implement a reasonably robust wireless network through multiple layers of security settings that adopt the checks-and-balances approach.

7.1 Comparison against commercial solutions

Recent advances in wireless networking technology, both on the hardware and software side, have recognized the need for security. The market has a variety of products and services on offer that aim to provide an integrated security solution for wireless networks, with minimal setup and end-user training.

However, procuring and deploying such commercial solutions is neither cheap, nor easy by way of effort. Hardware and software configurations, end-user training and administrative overhead are often significant and costly contributors to a delayed deployment.

In contrast, the steps detailed in this paper are intended to:

- Require minimal user training (administrator) and effort to deploy / procure
- Require minimal end-user training
- Require minimal system downtime
- Require minimal additional expense
- Educate the system administrator and end users about securing the wireless network rather than everything be transparently managed by a software / hardware solution
- Educate the system administrator on the various features of the wireless router that could help with troubleshooting

© SANS Institute 2005 Author retains full rights.

7.2 Salient features

The core advantages and disadvantages of this security model are summarized below:

7.2.1 Advantages

The most significant advantage of this security model is the transparency of the implemented security features to the end user. In addition:

- **For system administrators**
  - Automated intrusion detection alerts,
  - easy means to view the access logs in order to monitor for any unauthorized access and troubleshooting
  - no dependence on any client software since the router's administration is via a Web interface

- **For authorized and guest users**
  - Portable connectivity to the Internet and shared network resources within the network with transparent-yet-robust security safeguards

7.2.2 Disadvantages

Owing to the MAC address filter list and the restrictive DHCP lease; guest users will not be able to access the wireless network until they provide the system administrator with their MAC address, and get the WEP key from the system administrator or authorized user.

For a home office environment wherein there is a high frequency of guest users, this administrative overhead may prove to be a disadvantage.

7.2.3 Suggestions to maintain a secure wireless network

In conclusion, the following are some suggestions that could be easily deployed by the average home office wireless network system administrator to have a reasonable assurance in the security of the wireless network:

- The system administrator should frequently check the logs, both at the router and in an automated, always-on intrusion detection system like AirSnare
- The system administrator should restrict knowledge of the WEP key for the network to authorized individuals only
- The system administrator should restrict knowledge of the administrator password to a very limited set of authorized individuals only

© SANS Institute 2005 Author retains full rights.

References

Ewalt, David M.: 'Think You're Wireless? Think Again'; April 7, 2005; http://www.forbes.com/technology/wireless/2005/04/07/cx_de_0407mesh.html; 2005-04-09 18:22.

Bradley, Tony: Free Wireless Security; http://netsecurity.about.com/cs/hackertools/a/aafreewifi.html; 2005-04-09 18:27.

Script Kiddie: Wikipedia; http://en.wikipedia.org/wiki/Script_kiddie; 2005-04-09 19:49.

Moskowitz, Robert: WLAN Testing Reports – 'Debunking the Myth of SSID hiding'; December 1, 2003; http://www.icsalabs.com/html/communities/WLAN/wp_ssid_hiding.pdf; 2005-04-10 08:12.

Wi-Fi Protected Access: Wi-Fi Alliance; http://www.wi-fi.org/OpenSection/protected_access_archive.asp; 2005-04-10 07:30.

AirSnare: Digital Matrix; http://home.comcast.net/~jay.deboer/airsnare; 2005-04-10 08:21.

AirSnort: SourceForge; http://sourceforge.net/projects/airsnort; 2005-04-10 08:44.

WepCrack: SourceForge; http://sourceforge.net/projects/wepcrack; 2005-04-10 08:45.

D-Link: ANT24-0700 7 dBi Omni-Directional Indoor Antenna; http://www.d-link.com/products/?sec=1&pid=416; 2005-04-10 08:30.

D-Link: DWL-M60AT 2.4 GHz Directional Indoor Antenna; http://www.d-link.com/products/?sec=1&pid=58; 2005-04-10 08:30.

Symbol: 'Why Not Broadcasting SSID Is Not Secure'; March 25, 2003; http://www.symbol.com/products/wireless/broadcasting_ssid_.html; 2005-04-10 08:51.

© SANS Institute 2005 Author retains full rights.