




Wireless

Security Assessment



and the Deployment of I.D.S.

Group 16

**Stephen Barnett
Ben Bourne
Scott Clark
Paul Collinge**

5th March 2004

Project Definition

Students: Stephen Barnett
Ben Bourne
Scott Clark
Paul Collinge

Level of Project: BSC Computing (Networks and Communications)

Title of project: An investigation into Wireless Security Assessment and Deployment of Intrusion Detection Systems (IDS)

Elaboration This project consists of outlining IEEE 802.11 wireless technologies, security issues and recommendations. This includes recommendations for a secure Wireless Local Area Network (WLAN) deployment, an investigation into the security assessment of such a network and, an investigation into the use of IDS for continual security monitoring on both WLANs and traditional wired LANs.

Aim The aims of this project are:

- To analyse WLANs and their security features and issues so as to produce a recommendation for best practice WLAN deployment
- To analyse security assessment techniques and recommend those most suitable for a thorough assessment of a WLAN.
- To analyse the use of Intrusion detection systems as a way of monitoring the security of a WLAN.
- To incorporate all of the above findings into a set of recommendations for deploying, testing and maintaining a secure WLAN and traditional LAN.
- To produce an experiment for other students to learn about the areas investigated within the report.

Table of Contents

1.0 Introduction into Wireless Security	06
1.1 Introduction	06
1.2 Purpose of the Project	06
1.3 Research Methodology	06
1.4 Scope of Research	07
2.0 Defining Security	08
2.1 What is Security?	08
2.2 WLAN Standards	08
2.3 Security Benefits of Each Standard	10
2.4 WLAN Security Mechanisms	10
2.4.1 Introduction	10
2.4.2 Wired Equivalent Protocol (WEP)	10
2.4.2.1 WEP Authentication	10
2.4.2.2 WEP Confidentiality/Encryption	11
2.4.3 Virtual Private Network	12
2.4.4 WPA and RSN(802.11i)	14
2.4.4.1 WPA	14
2.4.4.2 TKIP	14
2.4.4.3 AES	14
2.4.4.4 802.1X	15
2.4.4.5 EAP	15
2.4.4.6 TLS over EAP (EAP-TLS)	16
2.4.4.7 Lightweight EAP (LEAP)	17
2.4.4.8 Protected EAP (PEAP)	18
2.4.4.9 Remote Access Dial-in User Service	18
2.5 What is Intrusion Detection?	19
3.0 Vulnerabilities of a WLAN	21
3.1 Introduction	21
3.2 Why are WLAN's Insecure?	21
3.3 Types of Attackers	21
3.3.1 Revenge Attackers	22
3.3.2 Profit Attackers	22
3.3.3 Inquisitive Attackers	22
3.3.4 Kudos Attackers	22
4.0 Types of Attackers on WLAN's	23
4.1 Attacks without Keys	23
4.1.1 Snooping / Eavesdropping and Network Monitoring	23
4.1.2 Modification (Man in the Middle Attack)	23
4.1.3 Masquerading (Spoofing)	24
4.1.4 Denial of Service	24
4.2 Password / Secret Key Attacks	25
4.2.1 Brute Force Attacks	25
4.2.2 Dictionary Attacks	25
4.2.3 Algorithm Attacks	26
5.0 WLAN Security Assessment	27
5.1 What is WLAN Security Assessment	27
5.2 Steps to Perform when Carrying out Security Assessment	27
5.3 Methods of Security Assessment and Testing Techniques	28
5.3.1 Wireless LAN Testing (War Driving)	28
5.3.1.1 Introduction and Description	28

5.3.1.2 Analysis of Wireless LAN Testing	30
5.3.1.3 Summary	30
5.3.2 Penetration Testing	31
5.3.2.1 Introduction and Description	31
5.3.2.2 Analysis of Penetration Testing	33
5.3.2.3 Summary	33
5.3.3 Honeypots	34
5.4 Wireless Networking Tools	38
5.5 Independent WLAN Security Auditors	39
6.0 Recommendations arising from a WLAN Security Assessment	41
6.1 Technical	41
6.1.1 PHY Standard	41
6.1.2 Security Protocol	41
6.2 Non Technical - Practical Recommendations	42
6.2.1 Change the default SSID	42
6.2.2 MAC Address Filtering	42
6.2.3 Password Folders and Files	42
6.2.4 Access Point Placement	42
6.2.5 Security Assessment	42
7.0 Ongoing Security Monitoring	43
7.1 Intrusion Detection Systems (IDS)	43
7.1.1 Types of IDS	43
7.1.1.1 Host Based IDS	44
7.1.1.2 Network Based IDS	45
7.1.1.3 Application Based IDS	46
7.1.2 How IDS Works	47
7.1.2.1 IDS Analysis	47
7.1.2.1.1 Misuse Detection	47
7.1.2.1.2 Anomaly Detection	48
7.1.2.2 IDS Responses	49
7.1.2.2.1 Active Responses	50
7.1.2.2.2 Passive Responses	51
7.1.2.3 IDS Reporting	52
7.1.3 Deployment of IDS	52
7.1.4 Commercially Available IDSs	54
8.0 Conclusions and Critical Evaluation	56
9.0 References and Bibliography	57
9.1 References	57
9.2 Bibliography	57
Appendices	60
Appendix 1 - IDS Practical Tutorial	60
Appendix 2 - WLAN Security Checklist	63
Appendix 3 - WLAN Security Summary	66

“Therefore, against those skilled in attack, an enemy does not know where to defend; against the experts in defence, the enemy does not know where to attack

Therefore I say: 'Know the enemy but know yourself; in a hundred battles you will never be in peril' "

- Sun Tzu, The Art of War

The above quote, although written many hundreds of years ago, is highly relevant in today's wireless world. A network administrator has to know his network inside out, in addition to knowing his attackers motives and methods to be able to properly defend his network.

Security analysis and intrusion detection systems are two tools essential to achieving this goal and as such will be investigated within this report.

1.0 Introduction into Wireless Security

1.1 Introduction

A Wireless LAN is normally implemented as an extension to an existing wired LAN in a corporate environment. It uses radio waves to transmit and receive the data that would normally travel along fixed wires. A wireless LAN therefore allows users to connect to the company network wherever they are, provided they are inside the coverage area.

Such networks have gradually gained popularity amongst both corporate and home customers since the initial Institute of Electrical Engineers (IEEE) specification 802.11 was released in 1997. This was the first internationally approved standard for wireless LANs. Numerous standards have been released since this initial one and improvements in capability, data rates and security have accelerated the uptake of WLANs as an integral part of computer networks.

Wireless networks provide greatly increased mobility and flexibility for mobile users, freeing them from the fixed location necessary when using a traditional wired LAN this in turn increases productivity and cost savings when compared to traditional wired LANs.

Network managers have the freedom to deploy extensions to their LAN in places not previously feasible such as Listed or hard to wire buildings, there is no need for extensive wiring or fixed access points in floors or walls. They can also be used to interconnect buildings without the need for laying cables.

One major factor that has held back the deployment of WLANs until recently is that of security. The security of a WLAN cannot be presumed secure in the same respect a traditional LAN can be.

1.2 Purpose of the project

In this paper we intend to look at ways of making a WLAN as secure as a wired LAN, ways of testing this security, and finally, ways of monitoring the security of the entire network to ensure the desired levels are continually assessed to ensure no breaches are present and allowing us to react quickly to any threat.

1.3 Research Methodology

The report will concentrate on achieving the aims set out earlier by utilising research papers, journals, online articles and software. The report then will then include the findings from the above research, in addition to the tools available in University laboratories to describe an experiment that will demonstrate the outcomes of the report in a practical manner to other students.

1.4 Scope of Research

It is necessary to provide an outline of the current 802.11 standards and security features so as to best achieve the goals set out for the report. However it is not within the scope of the report to provide detailed technical description of the workings of such areas. Therefore we will only focus in detail upon those areas deemed important enough to warrant such investigation.

With security assessment techniques and intrusion detection systems this is also the case, we will not provide a detailed technical assessment of the technologies, instead concentrate on the variety of tools available and their respective advantages and disadvantages.

2.0 Defining Security

2.1 What is Security?

It is a complex task to clearly define the word security; it is used in many different contexts and means different things to different people within those contexts. Edney and Arbaugh (2003) use a useful analogy to convey define security in the context we are looking at. They define security in the context of two groups: “the good guys” and the “bad guys”. If there are no “bad guys” then you are secure by default. Security tries to create a controlled space where there are no “bad guys” at a given time, and if security is implemented successfully, the entity being secured is immune to the influence of the “bad guys”.

In terms of Wi-Fi security we must ensure that we concentrate on all aspects of security to achieve this goal, this way we can be confident an attacker cannot interfere with or monitor any of our actions.

Bruce Schneier reinforces this statement saying “Security is a process not a product” We can’t ‘buy’ security out of a box, but we have to look at every process and ascertain its security risks, and then work to close that risk. This has to be done continually as a once secure system may not be so in time.

2.2 WLAN Standards

A Wireless LAN is normally implemented as an extension to an existing wired LAN in a corporate environment. It uses radio waves to transmit and receive the data that would normally travel along fixed wires. A wireless LAN therefore allows users to connect to the company network wherever they are, provided they are inside the coverage area.

Wireless LANs have gradually gained popularity amongst both corporate and home customers since the initial Institute of Electrical Engineers (IEEE) specification 802.11 was released in 1997. This was the first internationally approved standard for wireless LANs

Numerous standards have been released since this initial one and improvements in capability, data rates and security have accelerated the uptake of WLANs as an integral part of computer networks.

802.11 operates in the ISM bands (Industrial, Scientific and Medical bands)

There are four main specifications:

802.11 PHY	Max Data Rate	Frequency	Modulation
802.11	2Mb/s	2.4GHz and IR	FHSS and DSSS
802.11b	11Mb/s	2.4GHz	DSSS
802.11g	22Mb/s	2.4GHz	OFDM
802.11a	54Mb/s	5GHz	OFDM

Table 1.1 802.11 standards

802.11

The original 802.11 specification had low throughput and interoperability problems. A card that implemented 802.11 with DSSS could not communicate with a device that used FHSS 802.11. This standard is no longer in widespread use, it may still be apparent in some legacy systems within businesses and more likely, Wireless Home networks.

802.11b

The 802.11b specification, released in 1999 uses Direct Sequence Spread Spectrum (DSSS) in the 2.4 GHz range. It increases the transmission rate to a more acceptable 11Mb/s although this can scale down to 1Mb/s based on conditions.

After the interoperability problems that plagued the initial standard, the WLAN industry came together to create the Wireless Ethernet Compatibility Alliance (WECA) which certifies products that use the 802.11b protocol, this improved interoperability as any product with the Wireless Fidelity Mark (Wi-Fi) that the group gives certified products, will interoperate with any other device with the same mark.

802.11a

The 802.11a standard was released in 2001 and uses Orthogonal Frequency Division Multiplexing (OFDM) to provide data rates up to 54 Mb/s. 802.11a has many advantages over 802.11b, the higher bit rate is achieved by transmitting on sub frequencies in parallel which provides a greater resistance to interference. The standard can scale down to slower speeds if the conditions necessitate.

802.11g

802.11g was the fourth standard to be released and operates in the same 2.4 GHz range as 802.11b but provides higher data rates of up to 54Mb/s by using OFDM like 802.11a.

802.11g is backward compatible with 802.11b so an 802.11g wireless card can connect to an 802.11b Access Point (AP) and vice-versa. As with the other recent standards, the data rate can be reduced depending on prevailing conditions.

2.3 Security benefits of each standard

Regardless of the physical layer standard used, the security issues experienced by 802.11 networks are the same, no one standard has benefits over the other in terms of security. In saying this, some of the modulation techniques used are harder for an attacker to 'lock' onto than others, however with the right equipment this does not provide a big enough issue for an attacker, to warrant choosing one over the other for its security benefits.

2.4 WLAN Security Mechanisms

2.4.1 Introduction

As the data is transmitted through the air in a WLAN, it travels in insecure areas and therefore interception of the signals by an attacker is a very real threat. It is for this reason that encryption is used to try and make the signal unreadable by an attacker.

In this section we will look at the various security mechanisms currently available to provide transmission layer security within 802.11 culminating in a recommendation of the best option/s for deployment of a WLAN.

2.4.2 Wired Equivalent Protocol (WEP)

The original 802.11 Media Access Control (MAC) specification includes an encryption protocol called Wired Equivalent Privacy (WEP). As the name suggests, this encryption protocol is designed to give 802.11 networks the equivalent security as a traditional wired network. If this was to be the case, network managers could deploy wireless networks as freely as they would wired ones, safe in the knowledge that the security levels were the same as wired LANs. Unfortunately this is not the case and we will now take a brief look at why this is the case.

WEP was designed to give a wireless LAN two important security properties: authentication and confidentiality/encryption

2.4.2.1 WEP Authentication

This phase is to allow the following: If a wireless client wants to join an AP, it must first prove its identity and the AP should be able to check it is authorised to join the network before allowing it to do so. Ideally this should happen in reverse, i.e. the AP must authenticate itself to the client.

This is done in WEP by the use of the shared key, when a wireless device requests authentication, the access point sends it a 128-bit random number called a challenge text or a nonce. The client then encrypts this number with the shared secret key using WEP and returns it to the AP. Once decrypted, if the challenge text matches

the one sent originally, then the association was successful and the client is allowed to access the network.

Unfortunately the authentication stage used in WEP is so useless it actually aids an attacker in cracking the shared key, therefore it was completely dropped from the Wi-Fi specification. Below we briefly describe why this is so.

Firstly the key used to encrypt the challenge text sent by the AP is the same shared WEP key as is used for encryption.

Secondly the authentication method only attempts to authenticate the wireless client, the AP is not authenticated by the client.

Thirdly, after the initial authentication stage is successful, there is no subsequent authentication; the client is simply allowed to maintain its status on the network.

Finally, the initial authentication method requires the sending of a random value to the client, and the encryption of this with the WEP key. This means that any attacker monitoring the network now has the challenge plaintext, and its WEP encrypted version. The attacker can now very simply find out the RC4 random key stream.

This data, in addition to allowing the attacker to authenticate, assists him in cracking the encryption key so he can send messages when he is authenticated.

2.4.2.2 WEP Confidentiality/Encryption

When WEP is enabled on a WLAN, the data sent over it is encrypted so that any eavesdropper cannot understand the correct structure of the data.

This works by the use of a shared secret key, the receiving party can decrypt the data using this key.

To stop the same data from being encrypted to the same ciphertext each time it is encrypted, an Initialisation Vector (IV) is used to effectively change the key every time a packet is sent. The problem with this is that the IV is sent in the clear with each packet, so the attacker can collect these and notice when a value is used again, this allows a base for an attack.

The IV used in WEP is only 24-bits long; this number is not long enough as on an average system, all values would be used in around 4-7 hours. This problem is exasperated as many companies do not rotate their IVs so they are the same day after day.

The WEP key itself is either 40-bits or 104-bits; these values are no longer big enough to prevent trying all possible values (brute force cracking) on a modern pc. A modern pc can crack a 40-bit WEP key in under an hour, the 104-bit version does not provide a much greater level of protection, and this can be cracked in, on average just over double the time.

WEP keys are also susceptible to Direct key Attacks.

The method monitors the traffic and eventually can guess the first key byte; this continued over time allows the attacker to get the entire key. There are various freely available tools that utilise this weakness to break WEP keys at will. Some of which are discussed in section 5

It is a common misconception that by implementing WEP, you have a secure network by default. We have shown here in detail why this is not the case and as such WEP is not recommended as a security solution for 802.11.

The issues discussed, make it clear why WEP is unsuitable for use on WLANs, there are also administration issues with the protocol. Keys have to be distributed manually in WEP; this does not scale well, and carries a high overhead for the network administrator.

It is now a widely agreed fact that WEP does not live up to its name, it cannot be relied upon to secure a WLAN, Potter and Fleck (2002) state:

“WEP may raise the bar for an attacker but provides no real security from a determined attacker”

We will now look at an option that provided an interim solution to the inadequacies of WEP while the WPA and RSN standards were being defined; it is looked at in quite some detail as it is still an effective technology.

2.4.3 Virtual Private Network (VPN)

Virtual Private Networks (VPN) extend the trusted zone of a company LAN into an untrusted zone via the use of a secure tunnel. VPN uses a security protocol to form the tunnel, usually from a portable device to a company LAN. The data is encrypted, and as such it is safe to assume the data is impenetrable to any would be attacker in the untrusted zone the data flows through.

VPN is a complex and time consuming system to install and maintain it is therefore mainly found in larger corporate environments where they have the resources to manage the system. Client software needs to be installed on all connecting devices, and on any connecting servers at the other end. Some versions are incompatible with other vendors' versions so it is normally necessary to buy a complete package from one vendor.

“VPN is widely used in corporations for remote access and, in these applications, it is very effective” (Norris and Pretty 2000).

The VPN solution for WLANs is to treat the users as remote users when they are in fact, inside the office. This is done by encrypting the communications from a Wireless client with VPN software before it is sent over the network.

The communications travel to the AP, then to an Ethernet connection placed outside the firewall, then through the firewall to be decrypted by a VPN server. The data is then allowed onto the company LAN to arrive at its intended destination.

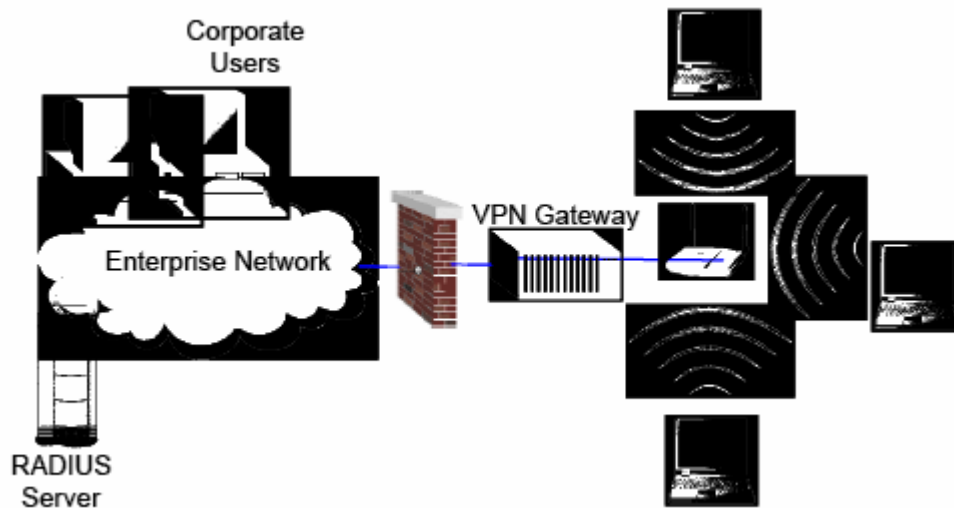


Figure 1 VPN Example

There are a number of obvious disadvantages and problems associated with using this approach:

- VPN software must be placed on the laptop trying to connect to the LAN. On older models this extra burden on the processor may degrade the performance of the laptop. This is not so much of a problem for newer models with fast processors and plentiful RAM, but many companies still use older laptops due to the cost of upgrading. This could increase the cost of installing an already costly solution.
- VPN servers generally have limited capacity, normally supporting between 20 and 50 users, if a company has an existing mobile user base then the extra load put on the server may be too much, a new high capacity (and high expense) VPN server will be required.
- As the WLAN must be separate from the existing LAN, new wiring and connection equipment must be purchased and installed to ensure the separation of the two networks. This adds to the initial cost of installation and increases the maintenance necessary.
- Enterprises using pre-shared keys for VPN connections will encounter the same scalability and key distribution that occurs when using WEP.

Due to the complexity and large set up costs, the VPN approach is generally used in large organisations that found using WEP was not viable and there was no real alternative. This approach will probably return to its remote access role once 802.11i (RSN) is fully ratified and tested. Using RSN or WPA is much cheaper and easier to install and administer and is much more viable for smaller businesses and home users.

That said, once the setup has been done, VPN does provide a robust secure method for securing a WLAN when there is no viable alternative.

2.4.4 WPA and RSN (802.11i)

WEP was originally designed to facilitate inherent security, as indicated by its name (Wired Equivalent Privacy) in that it was supposed to allow the same security as a traditional wired LAN. If this was the case there would be no problem with placing the WLAN inside the trusted zone of the LAN but as we discussed earlier, WEP failed to live up to its name.

This failure has prompted the IEEE to introduce a new security standard that can cope with these demands. IEEE 802.11i or Robust Security Network (RSN) is still being ratified and due for release in the second quarter of 2004. However an interim solution containing a subset of the final standard was released in April 2003, this was called Wi-Fi Protected Access (WPA).

2.4.4.1 WPA

The Wi-Fi alliance has taken a subset of the 802.11i standard, calling in Wi-Fi Protected Access (WPA) and began certifying products in April 2003.

This was done as the major Wi-Fi manufacturers realised that security was so important to end users that they had to quickly release a replacement for WEP. Wireless deployment had stalled due to the bad press WEP was receiving, however, manufacturers knew customers would not want to have to upgrade their new and expensive hardware, so the solution had to be in the form of a software update.

2.4.4.2 TKIP

WPA uses a new protocol called Temporal Key Integrity Protocol (TKIP) to improve the key security used with WEP by replacing the use of RC4.

TKIP is based on the same encryption algorithm as WEP, so it can reuse the existing RC4 encryption chips.

TKIP fixes the repeated IV problem WEP suffers from by doubling its size to 48 bits, and separating the IV from the key so that all 128 bits can be used for key data. Keys can also be assigned on a per user basis and changed whenever necessary rather than being shared by the entire network.

Another key is used for authentication of individual packets; this provides the facility to prevent an attacker from hijacking a user's session after login and masquerading as that user.

2.4.4.3 AES

TKIP is replaced in RSN by Advanced Encryption Standard (AES) which is currently the USA government's official cipher. This standard has been adapted for WLANs by adding a message integrity check (MIC) to each every packet and the standard is named AES-CCMP.

While TKIP was invented to quickly resolve the issues found with WEP, AES was designed from the ground up to provide a secure standard to completely replace WEP. Therefore when using AES as part of IEEE802.11i, users must purchase new hardware which supports this standard. IEEE 802.11i does allow TKIP to be used

by users of older hardware as an interim solution until they upgrade to new hardware supporting AES.

2.4.4.4 IEEE 802.1X

Access control was one of the major issues with WEP and the new security solutions WPA and RSN use a combination of IEEE 802.11, IEEE 802.1X, EAP and RADIUS to provide a solution to this problem.

IEEE 802.1X and Extensible Authentication Protocol (EAP) are mandatory for both WPA and RSN. RADIUS is the method of choice for WPA but is an option for RSN

IEEE 802.1x is designed to provide access control at the point where a client joins the network. This is done by protecting the ports where a user connects to the network, in the case of a WLAN every connection. The protocol limits the use of the port until such time that the client is authenticated. The protocol was also designed to provide secure key distribution and is used in both WPA and RSN.

The protocol used to communicate between the supplicant and the authenticator (in our case a wireless AP) is called EAP, which we will look at later. This protocol is also used between the authenticator and the authentication server. If the authentication server is in a remote location, as is normally the case with larger WLANs, then Remote Authentication Dial-In User Service (RADIUS) is used to transfer the requests over an IP network. Again we will look at this in due course.

With a wireless AP, each supplicant is given a logical port with an authenticator. When the supplicant wants to join, it is greeted by a locked port, it is asked for its authentication details (usually user name and password), these details are checked by the authentication server, and access denied or granted based on the outcome.

2.4.4.5 EAP

802.1x was based on a design used for use in dial-in networks, these networks use PPP connections, and EAP was designed to as an authentication method for such connections.

IEEE 802.1x LANs have no need for PPP as they are designed to send data packets. EAP was adapted for transport on 802.11 networks in the form of EAPOL (EAP over LAN).

This protocol has several additions including that of transferring key information. Its main goal is to pass messages between the supplicant and the authenticator.

As far as the authentication side of things is concerned, EAP supports many mechanisms including Lightweight EAP (LEAP), Protected EAP (PEAP) and EAP over Transport Layer Security (TLS). All of these options are complex however it is not within the scope of this report to look at these complexities, therefore we provide a short outline of each standard.

2.4.4.6 TLS over EAP (EAP-TLS)

TLS is not specifically designed for use in wireless networks, it is based on SSL which is widely deployed in web browsers and servers and is highly regarded. This method requires the use of a certification server to distribute and authenticate client certificates. The protocol provides: mutual authentication, integrity protected cipher suite negotiation and encryption key determination.

Davies (2003) describes EAP-TLS as the:

“Preferred authentication method for windows based wireless connectivity” when using user and computer certificates.

However Potter and Fleck (2002) state

“The downside of running an EAP-TLS infrastructure is the fact that you have to run your own certificate authority. For an organisation of any size, this is not an issue to be undertaken likely. There are many issues, technical and otherwise, involved in running a CA” (Certification Authority)

Therefore it can be summarised that although EAP-TLS provides a strong form of Authentication, it is only suitable for larger enterprises with the expertise and manpower to install and maintain the infrastructure.

2.4.4.7 Lightweight EAP (LEAP)

LEAP is a Cisco proprietary 802.1X authentication type for wireless LANs that supports mutual authentication between the client and a RADIUS server.

Although it is a proprietary standard it is widely used or supported by various vendors in RADIUS equipment.

LEAP provides the following benefits:

- Mutual Authentication
- Dynamic Session Key creation
- Centralised key management

However there are a large number of issues with LEAP as it was designed as an interim solution to WEP.

It can be concluded therefore that LEAP is no longer viable for use on its own, it was a major step forward in WLAN security when released but it has a number of flaws. The new standards have utilised areas of LEAP and improved on them to provide a much better solution which should be used where possible.

2.4.4.8 Protected EAP (PEAP)

Protected EAP (PEAP) is an 802.1X authentication type for WLANs. PEAP provides strong security, user database extensibility, and support for one-time token authentication and password change or aging.

The purpose of EAP is to provide authenticity, the purpose of PEAP is to provide this authenticity in a private way.

This is achieved by performing the EAP negotiation in a secure tunnel that is both encrypted and integrity protected with TLS.

PEAP is based on server-side EAP-TLS. This allows, organizations to avoid the hassle associated with installing digital certificates on every client machine as is required by EAP-TLS and instead select the method of client authentication, such as logon passwords or OTPs that are most suited to them.

2.4.4.9 Remote Access Dial-In User Service (RADIUS)

It is a common misconception that RADIUS is the name for an authentication server, while this may well be the case, RADIUS is in fact a widely deployed protocol which enables centralised authentication. The protocol was designed for TCP/IP networks and was initially used for authenticating dial in internet users, hence the name.

The RADIUS server is connected to a database of user information that it uses to verify the authentication credentials and obtain user specific account properties such as authorisation levels.

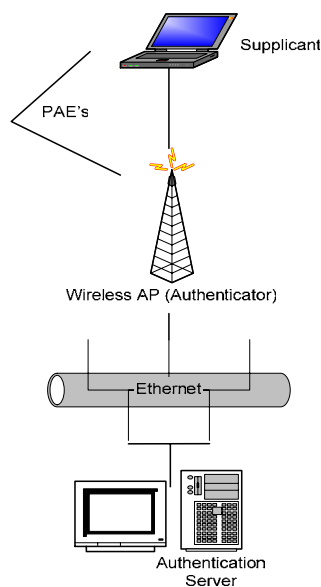


Figure 2 WLAN using an authentication server

Once the user is authenticated, the following transmissions need to also be authenticated to prevent a session hijacking attack. RADIUS does this on a per-packet basis, the server does this by passing a secret master key to the AP. All following transmissions are encrypted by this key and therefore session hijacking is not possible.

RADIUS is a solid, proven, secure authentication method which is a recommended option in WPA and RSN.

	WEP	WPA	802.11i (RSN, WPA2)
Cipher Algorithm	RC4	RC4 (TKIP)	Rijndael (AES-CCMP)
Encryption Key	40-bit	128-bit (TKIP)	128-bit (CCMP)
Initialisation Vector	24-bit	48-bit (TKIP)	48-bit (CCMP)
Authentication Key	None	64-bit (TKIP)	128-bit (CCMP)
Integrity Check	CRC32	Michael (TKIP)	CCM
Key Distribution	Manual	802.1x (EAP)	802.1x (EAP)
Key Unique to:	Network	Packet, Session, User	Packet, Session, User
Key Hierarchy	No	Yes	Yes
Cipher Negotiation	No	Yes	Yes
Ad-hoc (p2p)Security	No	No	Yes (IBSS)
Pre-authentication (Wired LAN)	No	No	Using 802.1x (EAPOL)

Table 1.2: Comparison of WEP, WPA and RSN

2.5 What is Intrusion Detection?

We have looked at the various security mechanisms available to us with the 802.11 standard, we will now introduce intrusion detection as a security mechanism, an area that will be look at in more detail later on in the report.

Heady et al (1990) defined an intrusion as: “Any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource.”

Intrusion Detection is the process of monitoring a computer system or network and analysing the events that occur within those areas for signs of intrusion. An intrusion is an attempt to circumnavigate the security precautions in place with the aim of compromising the integrity, availability or confidentiality of a computer or network. These intrusions can be instigated by attackers outside of an organisation via the Internet, from within an organisation by a user attempting to gain access to resources they are not authorised to or a user misusing resources they are authorised to access.

To combat this problem Intrusion Detection Systems (IDSs) are software or hardware products that automate the process of monitoring, analysing and preventing these attacks.

This area of security is currently experiencing extremely fast growth as companies realise the requirement for solid and ongoing network security. Computergram Weekly magazine recently reported that *“Inline intrusion prevention product revenue is poised for "astronomical growth" between now and 2006, when it will form a \$924m a year market”* A large part of this revenue will be derived from IT departments looking to add extra layers of defense to their problematic WLANs.

3.0 Vulnerabilities of a WLAN

3.1 Introduction

We have now seen the 802.11 standards, how they work, and the various security protocols and standards available to make them as secure as a wired LAN. In this section we will look at why WLANs need this extra level of security and what motives an attacker may have to perform such an attack. Knowing such details helps us to defend against the attacks.

3.2 Why are WLANs insecure?

By their very nature wireless communications are insecure. The fact that radio waves can go anywhere and be received by anyone within range has had a huge effect on society, the public can now receive TV and radio signals through the air with relative ease. This property, while a great thing for the receiver, can be a nightmare for the sender. If the sender wishes to control who exactly can use these signals and who cannot, then he faces a daunting task.

This property that a WLAN manager requires can be referred to as:

“Receive anywhere, without the wireless property of send to everyone” (Edney and Aurbaugh 2003)

These vulnerabilities of WLANs are present due to the inherently different physical layer methods of a WLAN when compared to a traditional wired LAN.

A wired LAN uses cables to carry the communication signal between sender and receiver, because the cables are normally run inside a secure building, and the communications are contained (to a large degree) inside the cable then they can be considered secure from attackers. The attackers are expected to focus their efforts at the point where the network converges with the Internet; therefore security is concentrated at this point in the form of firewalls and De-militarized Zones (DMZ).

In contrast, a WLANs communications are not privy to the same rules, an attacker has easy access to the communications on the WLAN. This allows him to analyse the data and possibly use this data to attack a protected (or not) network.

3.3 Types of Attackers

In this section we will look at the main reasons an attacker would attempt to compromise a WLAN, this so we can better understand the types of attacks outlined in section 4.

There can be many reasons a person decides to attack a WLAN, the fact is that a WLAN has become the easiest place for an attacker to penetrate a network. If he knows you have a WLAN, and is intent on compromising the network in some way, the WLAN will generally be his first point of call.

3.3.1 Revenge Attackers

Revenge is a powerful motive for an attacker which is why this type of attack is becoming more common. Revenge attackers can come in the form of disgruntled former employees or non employees who have a grudge to bear with the company.

Former employees are the more dangerous of the two; they are more likely to know information to aid them in an attack such as Access point location and user names and passwords. Another issue is that revenge attackers will more than likely plan their attack over time and therefore make it more effective. Attacks such as this are meant to be visible and cause some kind of annoyance or loss to the company. They can come in the form of a Denial of Service (DOS), data deletion/corruption or virus release. A honeypot network which is discussed in section 5 provides a good deterrent to such an attack however.

3.3.2 Profit Attackers

Profit attackers work in a very similar way to revenge attackers, with one key difference, their aim is to remain undetected and make a profit from the information obtained from the attack. Such profit could come from data theft, which could be sold to a competitor (or back to the same company for cash), stock market knowledge or from the modification of data such a payroll info to make the attacker money. Like revenge attacks, profit attacks will more than likely be planned over time and therefore be more effective and harder to detect. Again, honeypot networks can be use to useful effect to scare off profit attackers by making them aware they have been detected.

3.3.3 Inquisitive Attackers

Inquisitive attackers form the most common type of attack upon a WLANs, the attacker normally has no specific reason for attacking the WLAN other than to see if he can. WLANs with little or no security are most at risk of such an attack, a 'war driver' can roam a neighbourhood scanning for unprotected WLANs and when he finds one, he can then do as he pleases with it. However with a moderate level of protection, most inquisitive attackers will simply pass on by and search for an easier target.

3.3.4 Kudos Attackers

This type of attacker forms the least likely attacker, but also the most dangerous. Members of the hacker community try and hack into networks in order to prove their credentials to other hackers. They will often have a great deal of knowledge and the best equipment and tools possible. Therefore a high level of security is required on WLANs (and other parts of the network) to keep out this type of attacker. Stories of people breaking into the FBI computer system are good examples of such attacks and go a long way to show just how hard it is to fully protect a computer network.

4.0 Types of attacks on WLANS

Wireless networks are vulnerable to a number of different types of attack. It is important that these are taken into consideration when thinking of designing and implementing a wireless network. The following sections aim to outline some of these methods of attack and potential security risks.

Edney and Arbaugh (2003) state there are four main classifications of attack: snooping/eavesdropping, modification, masquerading and denial of service. We will look at these areas in two terms, attacks without keys and attacks on the keys.

4.1 Attacks without Keys

The first area we will look at is those areas that can be achieved without having to know the encryption keys, later we will look at ways in which an attacker can obtain the keys.

4.1.1 Snooping/Eavesdropping and Network monitoring

The potential for unauthorised users to eavesdrop on wireless traffic is one of the main threats to a wireless network infrastructure. This is due to the fact that it is so easy because wireless communications are not confined to physical area, an attacker can simply sit in a car park outside the office, and eavesdrop on the network. Eavesdropping is a passive attack. Using wireless packet sniffers, attackers are able to analyse packets that are sent between a station and an access point, this can be done in real time, or by storing the data and analysing it at a later time. It is clear therefore that the privacy of sensitive information will be at risk in a wireless network, and it is entirely possible that the sender and receiver will not have any inclination that this invasion of privacy has taken place.

Some companies may not care that an unauthorised person can monitor their traffic, it may not be confidential, or of any use to anyone else. However, eavesdropping can lead to unauthorised access to the network, with obvious consequences; from free internet access for the attacker, to information deletion or virus insertion. It is clear therefore that allowing passive listening can lead to an active attack on the network.

Snooping is usually a passive first step to a more dangerous active attack.

4.1.2 Modification (Man in the Middle Attack)

These types of attacks involve an attacker intercepting the wireless transmission between two parties and assessing and modifying that data in such a way that the receiver/s do not realise that any modification has taken place.

This is normally done using a method called 'store and forward'. As it is hard to modify transmissions in real time, this is the most common method. An attacker captures the transmission, modifies it and then sends it on to its intended destination.

The attacker can either do this by intercepting the messages in the air and corrupting the original before it meets the AP, causing it to drop the packet/s, modifying the message and sending it on its way.

A more common and easily implemented method is to set up a bogus AP which acts as an intermediary between the client and the real AP, allowing easier message modification.

There is relatively little an attacker can do with this method if he does not know the encryption key used, he can however modify the destination IP address or replay messages for his advantage to capture login passwords and secret keys.

This type of attack is feasible as the early standards only required one way authentication, i.e. the AP authenticates the client but this is not done in reverse. Using WPA and RSN does solve this problem as both require two way authentication, and as such will spot a bogus AP.

4.1.3 Masquerading (Spoofing)

This method is used to trick an AP into thinking the attacking device is an authorised station. If such an attack is successful, the attacker can enter the network undetected and also have the privileges of an authorised device. Some WLANs use MAC address filtering as a way of authenticating clients as described earlier, an attacker can simply copy this MAC address and use it on his own device to access the WLAN. The more sophisticated techniques used by the latest WLAN standards make this type of attack much more difficult, and impossible in some cases.

4.1.4 Denial of service

Denial of service attacks are unlike any other in that they actively attempt to block out everybody (including the attacker) from the network. There can be many reasons for such an attack but ultimately the same goal, to cause damage to the target by disrupting its business through the disabling of its network.

The use of this tactic was demonstrated graphically recently through the use of the Mydoom and Doomjuice worm. The worm's purpose was to launch a denial of service attack against a software company called SCO (Santa Cruz Operation in the USA) which is involved in a dispute over ownership of an operating system - a rival to Microsoft Windows.

Although this example is not quite relevant to WLAN vulnerabilities, it is a good example to show the reasons for, and effects of a DOS attack.

In a WLAN a DOS attack may well take place in the form of flooding the AP with traffic, to deny any user access to it. But WLANs can provide access to a corporate network, access which an attacker can use to perform a DOS attack against a company web server for example, or a file server. This type of attack could be carried out by a competitor, a malicious hacker looking for 'kudos' or a disgruntled former employee, whatever the case, a DOS can be devastating to a company, and unfortunately are very hard to defend against, especially in a WLAN.

If an attacker knows what frequency range the WLAN is using (and he almost certainly will), it is easy to flood the frequency with noise to reduce the signal-to-noise ratio to a level where it is unusable. This is as the clients (and the AP) will be unable to distinguish the valid network data from the noise from the attacker.

Neither WPA nor RSN can prevent DOS attacks as the IEEE 802.11i task group decided that DOS was a fact of life and was not feasible to tackle in WLANs.

4.2 Password/Secret key attacks

There is only so much an attacker can achieve by attacking a WLAN without knowing the keys used for encryption, it is therefore obvious that an attacker might try and compromise the keys to achieve his goal. In this section we will look at possible methods for an attacker to do this.

4.2.1 Brute Force Attacks

The basis of a brute force attack is to try every possible combination of a key until the key is found. Obviously the complexity of such an attack is related to the size of the key, i.e. the longer the key used the longer the time necessary for a brute force crack. WEP originally specified a 40-bit key as this was the standard allowed for export from the US at the time. The failings of the WEP key were discussed earlier, highlighting the fact that a 40 bit WEP key can be cracked by modern equipment in under an hour.

Larger keys are also susceptible to the problem, but obviously take longer to crack. The ideal situation is to use a key where it is computationally impossible to crack via brute force i.e. it will take much too long using current pc standards. This is entirely feasible and it is now common for keys to be 256-bits and higher, such keys would take billions and billions of years to crack using this method. Therefore other methods must be used when the key is so large.

4.2.2 Dictionary Attacks

One such method is the dictionary attack, in this method an attacker would use a compiled dictionary of English words, dates, phone numbers, pet names, places etc to use to try and attack the key. The reason for this is that commonly passwords are easily remembered strings such as those described above. By trying only these common strings an attacker can crack a weak password in much less time than it would take using a brute force attack.

Modern techniques of obscuring the password make this type of attack ineffective, however there are still many systems in use where it is highly effective. This is the reason that most security aware network managers insist on random, varying case passwords.

4.2.3 Algorithm Attacks

If both brute force and dictionary attacks prove unsuccessful then the only option is to find a weakness in the actual algorithm used. This is not easy as most algorithms are designed to provide security and so are difficult, if not impossible to compromise, however this is not always the case.

As discussed earlier, the WEP algorithm was broken as it allowed one bit of the key to be cracked at a time, eventually the whole key would be known. This meant that most users of WEP who had increased the key size to 104-bits from 40-bits to offset brute force cracking, this offered little extra protection as it only slightly increased the time needed to extract the key.

Tools are now available that exploit the known weakness in the WEP protocol in a matter of hours, often less. This has the resulting effect of rendering WEP useless.

No self respecting network manager would use WEP for security, knowing full well a simple piece of software operated by a novice could compromise his network in under an hour.

This fact goes to show that once an algorithm is compromised, it is from then on rendered useless. Replacements for WEP such as WPA and RSN are designed to make such a compromise impossible, but then again so was WEP. Using the most up-to-date methods and continually auditing your network is the only way to stay one step ahead of an attacker. The next section will look at how we assess the security of our network once it is installed, in section 7 we look at Intrusion Detection Systems as a method of continually monitoring security.

5.0 WLAN Security Assessment

5.1 What is WLAN security assessment?

A WLAN Security Assessment ensures that the Wireless Local Area Network complies with effective security policies. A Security Assessment is necessary regardless of whether or not the network implements effective security mechanisms. It is important not to put too much trust in the design of a system. Tests should always be run to make certain that the network is hardened enough to guard against unauthorised persons attacking company resources.

Regular, periodic security assessments should be conducted to ensure that changes to the WLAN do not make the system vulnerable to hackers. A review once a year is acceptable for low risk networks, but a review at least each quarter or more may be necessary if the network supports high risk information (e.g. confidential government budgets or personal data etc).

5.2 Steps to perform when carrying out Security Assessment:

- (1) Review existing security policies
- (2) Review the system architecture and configurations
- (3) Review operational support tools and procedures
- (4) Interview users
- (5) Verify configurations of wireless devices
- (6) Investigate physical installations of access points
- (7) Identify rogue access points
- (8) Perform penetration tests
- (9) Analyse security gaps
- (10) Recommend improvements

5.3 Methods of security assessment & testing techniques

5.3.1 Wireless LAN Testing




5.3.1.1 Introduction and Description:

Commonly known as War Driving, this can be defined as "Driving around looking for wireless networks".

This method of Wireless LAN Testing is carried out by moving round an area with an antennae, amplifier and laptop. Although this method is often used as a testing method by auditors for the sole purpose of analysing their network, it should be noted that any hacker can easily adopt this method as well. Indeed antennae as basic as a Pringles Crisp tube have been used in the past with surprisingly effective results!

"People have made these antenna out of Pringles tubes, coffee cans and even old satellite dishes" (Geoff Davis, i-sec).

Once a hacker has discovered an open WLAN, they may mark the street with details of the access provided. This is called War Chalking.

let's warchalk..!	
KEY	SYMBOL
OPEN NODE	ssid  bandwidth
CLOSED NODE	ssid 
WEP NODE	ssid access contact  bandwidth
blackbeltjones.com/warchalking	

This diagram represents the different symbols used to identify WLAN's and their status. It enables people to see what wireless access points are in the area and what access they provide.

Organisations need to test their networks periodically for unauthorised and/or misconfigured wireless LANs. They should also scan their sites for incoming signals from neighbouring wireless LANs. Organisations can improve and speed up the auditing process by creating more than one portable computer with network cards and testing tools for detecting wireless LANs.

The frequency required for testing wireless networks will depend on the following factors:

- The physical location/factors of the location to be tested. (If the building is located thousands of metres from any public access area, then it will clearly not need to be tested as often as an office located in a busy city).
- The threat level faced by the organisation.
- What control the organisation has over its network resources. (e.g.: an organisation with tight central control over the network may need to be tested less often than with a much decentralised network support structure).
- How sensitive is the data that the company is passing. Clearly a credit card company would be more interesting to a hacker than a florist shop.

Organisations with high risks and threats should test for unauthorised and/or misconfigured wireless LANs on a monthly basis or more often. Random audits are also recommended.

5.3.1.2 Analysis of Wireless LAN Testing (War Driving)

Advantages:

- This technique of hacking is incredibly easy to do; all a person needs is an antenna, an interface card and a laptop computer. It is worth noting that antennae can be made from such basic things as Pringles crisp tubes!
- War driving can get quick results on Access Point locations and give the user a very quick and accurate outline of businesses' network security.
- There are a large number of War Driving pieces of software making analysis of networks easier and proving a rich set of varying results.

Disadvantages:

- Scanning entire network indiscriminately (Could be slow on large networks).
- Intrusive and noisy. There are plenty of networks around which will have Personal Firewalls and IDS alerts, making war driving a lot more difficult in these circumstances.
- War Driving can give "False Positives"; it is only a partial solution to testing Wireless Security.

5.3.1.3 Summary:

War driving is essentially used by hackers and generally destructive people. However it can be used to "fight fire with fire" and allow organisations to adopt the technique to see their own weaknesses from the outsiders perspective, thus it does have its uses.

5.3.2 Penetration Testing

5.3.2.1 Introduction and Description:

Penetration testing is a form of security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation. The purpose of penetration testing is to identify the methods of gaining access to a system by using common tools and techniques used by attackers. This type of testing should only be performed after careful consideration, notification, and planning.

Although penetration testing is an invaluable technique to an organisation's information security program, it is a very labour intensive activity and can require great expertise in order to minimise the risks to targeted systems.

Penetration testing can be "Overt" or "Covert". These two types of penetration testing are commonly referred to as Blue Teaming and Red Teaming.

Blue Teaming involves performing a penetration test with the knowledge and consent of the organisation's Information Technology staff.

Red Teaming involves performing a penetration test without the knowledge of the organisation's IT staff but with full knowledge and permission of senior management.

Some organisations designate a trusted 3rd party for the Red Teaming exercise

Penetration Testing consists of four phases (Figure 3):

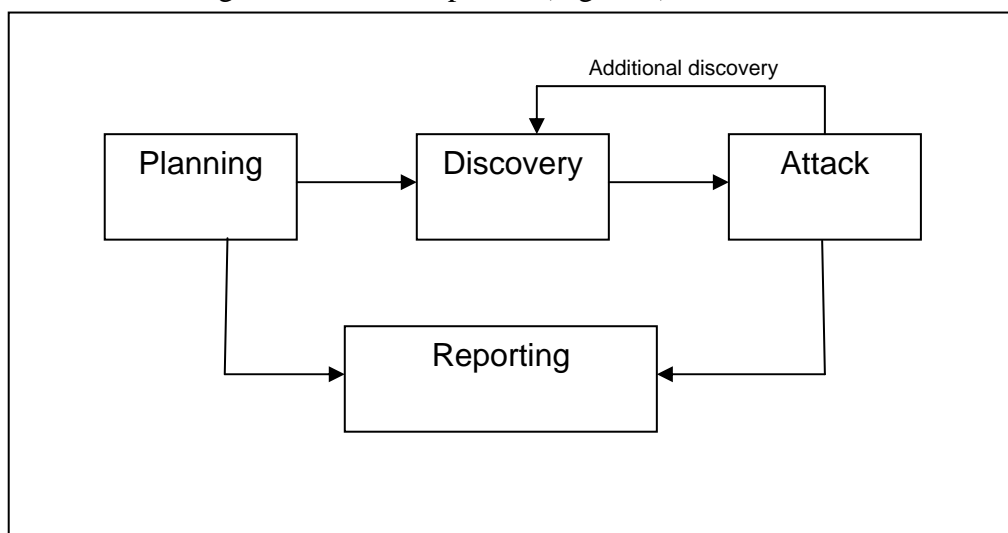


Fig. 3: Four-stage penetration Testing Methodolgy

Planning:

In the planning phase, rules are identified, management approval is finalised, and the testing goals are set. The planning phase sets the groundwork for a successful penetration test. No actual testing occurs in the planning phase.

Discovery:

The discovery phase starts the actual testing. Network/Port scanning is used to identify potential targets. In addition, other techniques are also used, such as: DNS interrogation, InterNIC queries, observation of organisations target web server(s), the searching of the organisations Lightweight Directory Access Protocol servers, Packet capture, NetBios enumeration, Network Information System studies and Banner grabbing. Vulnerability analysis is also looked at. During this phase, services, applications, and operating systems of scanned hosts are compared against vulnerability databases. It is generally better to carry these tests out manually, however it is a lot slower than using an automated scanner.

Attack:

Executing an attack is at the heart of any penetration test. It is here that previously identified potential vulnerabilities are verified by attempting to exploit them. If an attack is successful, the vulnerability is verified and safeguards are identified to mitigate the associated security exposure.

Reporting:

The reporting phase occurs simultaneously with the other 3 phases of the penetration test. In the planning phase, rules of engagement, test plans and written permission are developed. In the discovery and attack phase, written logs are usually kept and periodic reports are made to system administrators and/or management.

5.3.2.2 Analysis of Penetration Testing:

Advantages:

- The advantage of using Penetration testing is that it is ideal for testing detection and response capabilities. These tests provide a great opportunity to gain experience in a consequence-free exercise.
- Penetration tests are a fantastic tool for determining the current security position of an organisation. Often, as part of a routine, a Penetration test will be ordered to get a quick understanding, or “snapshot”, of problem areas in an organisation. The results can then provide direction on allocating limited resources.

Disadvantages:

- A typical penetration exercise is not a comprehensive evaluation of security, since many security issues and configuration problems may not be identified. If the fact that Penetration testing can be limited is misunderstood, the exercise can give an organisation a false sense of security.

5.3.2.3 Summary:

Penetration testing is only as good as the people conducting it. The difference between identifying potential vulnerabilities and gaining interactive remote access to hosts requires a huge increase in skill level. Commercial vulnerability scanners and free information-gathering tools provide the average systems administrator with the ability to identify potential vulnerabilities. Exploiting those vulnerabilities, escalating privileges and moving vulnerabilities in a complex, varied network environment requires highly skilled, experienced individuals. Teams with assorted, complementary skill sets usually perform the best penetration tests.

The future of Penetration testing is at the application level. Most organisations have or plan to deploy e-commerce related applications.

5.3.3 Honey pots

What is a Honey pot?

The first step in understanding honeypots is to define what a honeypot is.

Unlike firewalls or Intrusion Detection Systems, honeypots do not solve a specific problem. Instead, they are a highly flexible tool that comes in many shapes and sizes.

They can do everything from detecting encrypted attacks in IPv6 networks to capturing the latest in on-line credit card fraud. It is this flexibility that gives honeypots their true power. It is also this flexibility that can make them challenging to define and understand. As such, the following definition can be used to define what a honeypot is:

A honeypot is an information system resource whose value lies in unauthorised or illicit use of that resource.

This is a general definition covering all the different manifestations of honeypots.

Conceptually almost all honeypots work the same. They are a resource that has no authorised activity; they do not have any production value. Theoretically, a honeypot should see no traffic because it has no legitimate activity. This means any interaction with a honeypot is most likely unauthorised or malicious activity. Any connection attempts to a honeypot are most likely a probe, attack, or compromise.

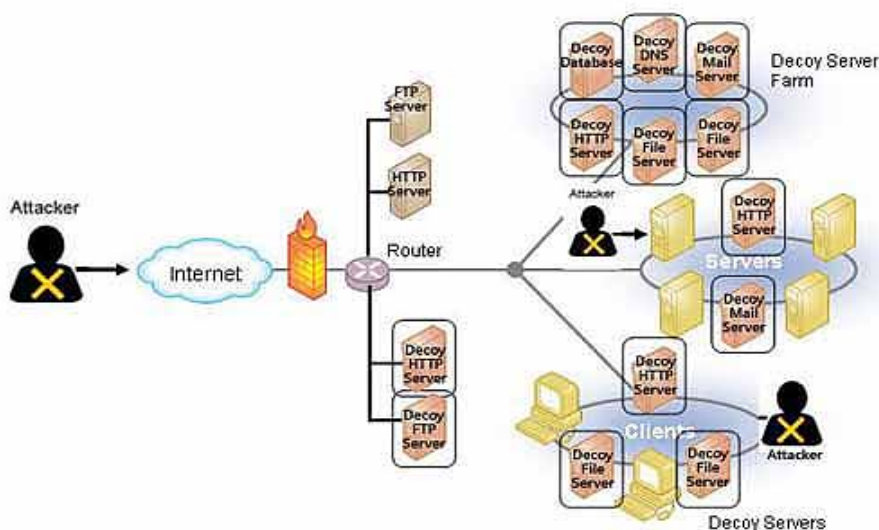


Figure 4: The layout of a honeypot, with decoy servers waiting for a blackhat to access.

A wireless honeypot could simply be a wireless resource that would wait for attackers or malevolent users to come through on your wireless infrastructure.

How do Honeypots work?

The way that a honeypot works is to emulate a machine, or an entire network, providing services and access. Instead of providing real services, they log access attempts to them, providing the maintainer with an insight into the tools and methods used to attack a system.

Wireless honeypots could help to reveal real statistics about such attacks on your infrastructure, such as the frequency of attacks, the attacker's skill level, his goals and methods. Wireless honeypots can also help with protecting your networks while the attacker expends significant effort on fake targets; thus with honeypots, blackhats will lose time in their discovery of your network.

Types of Honeypots

Interaction defines the level of activity a honeypot allows an attacker.

Low-interaction honeypots have limited interaction; they normally work by emulating services and operating systems. Attacker activity is limited to the level of emulation by the honeypot. The advantage of a low-interaction honeypot is their simplicity. These honeypots tend to be easier to deploy and maintain, with minimal risk. Usually they involve installing software, selecting the operating systems and services you want to emulate and monitor, and letting the honeypot go from there.

This plug and play approach makes deploying them very easy for most organisations. Also, the emulated services mitigate risk by containing the attacker's activity, the attacker never has access to an operating system to attack or harm others.

The main disadvantages with low interaction honeypots is that they log only limited information and are designed to capture known activity. The emulated services can only do so much.

High-interaction honeypots are different; they are usually complex solutions as they involve real operating systems and applications. Nothing is emulated; we give attackers the real thing. If you want a Linux honeypot running an FTP server, you build a real Linux system running a real FTP server. The advantages with such a solution are two fold. First, you can capture extensive amounts of information. By giving attackers real systems to interact with, you can learn the full extent of their behaviour, everything from new root kits to international IRC sessions, Many blackhats will install an IRC Bot on an infected machine, the main reason is to maintain a connection to their favourite IRC server. The second advantage is high-interaction honeypots make no assumptions on how an attacker will behave. Instead, they provide an open environment that captures all activity. This allows high-interaction solutions to learn behaviour we would not expect.

The way to design a wireless honeypot is to think about the kind of attacks that could occur and to develop an action plan.

First, attackers will scan for wireless networks, so you should send out fake packets, asserting the presence of a WLAN.

Or, you may be interested in deploying fake wireless resources dedicated to some honeypot infrastructure. Simulating traffic can be a more important issue on a wireless network dedicated to honeypot activity than on a wired one, because attackers need to see traffic in order to perform some of their attacks. Bypassing 802.1X, bypassing MAC address filtering, cracking malformed WEP keys, looking at beacons, looking at SSID in the frames used for connection by clients, and so on all require existing traffic to be analysed.

You will first need at least one device that offers wireless access. If you choose to use a real Access Point, then you can safely plug it on a wired network (with at least one computer) with visible resources playing the role of targets on this fake network, and invisible resources to record data and detect intrusions (data capture).

To monitor wireless-specific layer 2 attacks, one can use data capture on a wireless invisible client in mode Monitor, using software such as Kismet, which is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic.

Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of non-beaconing networks via data traffic.

Another option could be the use of wireless clients on such architecture. Usually, people deploying honeypots propose servers, but clients can be used to improve the realism or to monitor specific attacks. More specifically, on a wireless environment, clients can be used to simulate wireless traffic and also monitor layer 2 attacks and probes. In fact, some attackers listening to the wireless network traffic will recognise the presence of clients.

Sometimes, those clients are not well configured and badly protected (such as laptop used from home and brought to a company) and become interesting, easy targets.

As an example, an attacker could try to use a Rogue Access Point with a stronger wireless signal than the official wireless AP. A typical client will then automatically connect itself to the attacker's rogue access point and specific, evil actions can then be tried by the attacker: man in the middle attacks, denial of service, and infection with a new worm that spreads itself on the rest of the legitimate network after the client reconnects itself, and so on.

To look at easier solutions, one can also turn a wireless card in Master mode to simulate an Access Point, so that the honeypot is concentrated on only one computer. This is really cheap and easy to manage. Even if the honeypot is compromised, you should not have any problem if it's disconnected from your real network. Moreover, this computer could be either a high-interaction honeypot or a low-interaction honeypot.

Wireless honeypots suffer from the same stealth problems that classic honeypots do, and also from specific, additional ones related to this environment. Remember that skilled attackers may be afraid of "too open" networks. So, the rules of the game are easy:

- The better you simulate reality, the more you'll catch skilled attackers (but in this case, intrusions rarely occur);
- The less you deal with stealthiness, the more you'll see successful attacks (but they are often done by 'kiddies' or inexperienced attackers).

Therefore, depending on your goals, you might create honeypots with or without these options:

- Beacon transmission;
- WEP (or more generally, ciphering, that can be cracked more or less easily);
- MAC filtering;
- 802.1X authentication;
- Wireless traffic between clients and AP;
- Wireless clients with auto-connect mode enabled;
- Wireless networks using well known standards (802.11b, 802.11g and 802.11a?).

This new kind of security resource could easily become an effective way to monitor wireless intrusions attempts and to understand a blackhat's goals and their corresponding tools. Whether these people are corporate attackers, bandwidth borrowers, or cyber terrorists, they will be discovered.

Honeypots can be used for production purposes by preventing, detecting, or responding to attacks. Honeypots can also be used for research, gathering information on threats so we can better understand and defend against them in the future.

5.4 Wireless Networking Tools

Tool	Capabilities	Linux/Unix	Win32	Cost
Aerosol	Wireless Sniffer	NO	YES	Free
<i>Description: Aerosol is a freeware wireless LAN sniffer tool, which can also crack WEP encryption keys. Aerosol operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.</i>				
AirSnort	Wireless Sniffer	YES	NO	Free
<i>Description: AirSnort is a freeware wireless LAN sniffer tool, which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.</i>				
Kismet	Wireless Sniffer	YES	NO	Free
<i>Description: Kismet is an 802.11b wireless network sniffer. It is capable of sniffing using almost any wireless card supported in Linux.</i>				
Netstumbler	Wireless Sniffer	NO	YES	Free
<i>Description: Netstumbler is an 802.11b tool that listens for available networks and records data about that access point. A version is available for the Pocket PC.</i>				
Sniffer Wireless	Wireless Sniffer	NO	YES	£££
<i>Description: A Sniffer Wireless is a commercial wireless LAN sniffer that provides network monitoring, capturing, decoding, and filtering capabilities.</i>				
WEPCrack	WEP encryption cracker	YES	NO	Free
<i>Description: WEPCrack is a tool that cracks 802.11 WEP encryption keys using the latest discovered weakness of RC4 key scheduling.</i>				
WaveStumbler	Wireless Network Mapper	YES	NO	Free
<i>Description: WaveStumbler is a freeware console based on 802.11 network mapper for Linux. It reports the basic wireless network characteristics including channel, WEP, ESSID, MAC etc.</i>				

5.5 Independent WLAN Security Auditors:

An Independent WLAN Security Auditors are companies who provide their client organisation(s) with an opinion on that organisations WLAN security, but who are not otherwise affiliated with that organisation. The auditors use similar techniques to those discussed in order to produce an informative report on the state of a particular organisations WLAN security.

The auditors use the same methods as hackers to try to access your WLAN. First off, they try to find the characteristics of the LAN, is it open or closed? Is WEP active or not? Is WPA enabled? Is access filtered by MAC address?

If access is filtered by MAC address, MAC addresses can be spoofed to grant access. If WEP is active does it use a default key? If it doesn't, the key can be broken in a few minutes on a busy network.

Once the auditor has access to the network, they will see what services are on offer. As the airwaves are a shared medium, anybody with access to the WLAN can read all the packets, even if they are not destined for them. The auditor will check for the presence of a VPN, using a VPN ensures that data between two machines is encrypted and is unable to be read by anybody else.

Some example auditors are listed below:

(i) MATTA Assessment Services

MATTA are an independent Information Risk Management company. MATTA provide audits through best practice wireless scanning and security assessment tools and hardware with hands-on vulnerability qualification and reporting. MATTA provides its clients with a comprehensive wireless security assessment service.

(ii) OLOSEC

OLOSEC's practice is network and information security assessment. OLOSEC offers a comprehensive set of assessment services available anywhere, including assessment of compliance with government regulations. They utilise a risk-based assessment methodology that offers their clients clear perspectives on security threats, vulnerabilities, risks and priorities.

(iii) OCS

From ISP services to Technology Consulting and Systems Integration, OCS has a 15 year history of providing IT services to Small Businesses which gives them the experience to back up their commitment to their clients.

With OCS you are hiring a team; problems can be escalated to a more senior level consultant or routed to someone who has experience with the specific technology or issue. You may experience a problem or want to implement a technology which is outside the scope of knowledge of one person. The technology industry is too large a subject area for 1 individual to be an expert in everything.

OCS allows its clients to do what they do best; run their business. They focus on the technology infrastructure so that their clients don't have to. OCS offers a comprehensive suite of services for the small business. This eliminates wasted time and finger pointing between disjointed vendors which reduces overall costs.

(iv) Vanguard Integrity Professionals

They offer a complete wireless security assessment and a controlled penetration test. This is an example of Ethical Hacking. Ethical Hacking is where you hire somebody to try and hack into your computer system, reporting what they find.

6.0 Recommendations arising from a WLAN security assessment

Having outlined the different versions of 802.11, including the security options and flaws in the standard, and security assessment techniques we can now make a recommendation for installing and maintaining a secure wireless network.

We will do this in two steps, specifying technical recommendations and then non technical ones that need to be considered also.

6.1 Technical

6.1.1 PHY Standard

The actual standard selected for an 802.11 network (a, b, and g) do not have any effect on the security of the network. A survey should be conducted to find the most suitable standard for the purpose required. That said the original 802.11 standard should not be considered as it is no longer viable as a solution.

6.1.2 Security protocol

As discussed in section 2, WEP was the original security protocol issued with the 802.11 standard, and as discussed was fundamentally flawed. Therefore it is recommended that it is not used in any way to secure a WLAN, even a home WLAN. If an existing WLAN is to be used, then it is recommended to upgrade (normally by software updates to the client and AP) to WPA.

WPA contains a subset of the new RSN standard and patches all known security holes prevalent in WEP.

For new networks it is highly recommended that installation is stalled until the IEEE 802.11i standard (RSN) is ratified and released in the third quarter of 2004. As discussed previously, 802.11i provides a robust security layer for WLANs and one that is, as yet, unbreakable when configured correctly. The standard has been designed not to fail as WEP did, and has been thoroughly peer tested and reformed throughout its specification.

If it is not feasible to wait for this length of time then it is recommended to install WPA standard equipment, and upgrade when necessary. If security is not required to be at a high level, e.g. home networks, non sensitive businesses, then it may not be necessary to upgrade unless a major flaw is found in the WPA standard. IEEE802.11i can be supported in most new equipment by dropping AES in favour of TKIP, this can also be an option which improves on WPA if deemed necessary. The choice of 802.1x/EAP standards should be defined during a site survey and chosen to best protect the network while providing the necessary support for existing equipment and standards.

Use of a VPN should no longer be necessary except in those companies that have an existing infrastructure to support such a WLAN, WPA and RSN provide as good, if not better security than VPNs .

6.2 Non Technical - Practical Recommendations

6.2.1 Change the default SSID

By changing the default SSID of an AP to a random value, we can make it harder for an attacker to identify his target network. In addition to this, changing the default SSID has the effect of removing the blatant details of the make and model of the AP which are afforded to an attacker if the default manufacturers SSID is kept. Such details can be discovered quite easily, but by doing this we make life just that little bit harder for an attacker, and may well deter attackers looking for an easy target.

6.2.2 MAC address filtering

By only allowing a subset of MAC addresses access to the AP we can make life harder for any attacker. Although this can be worked around quite easily using MAC spoofing, it will deter attackers that are looking for an easy target.

6.2.3 Password folders and files

By insisting on the use of strong passwords we can raise the bar for an attacker once again. Long, multicas, non dictionary passwords can remove the risk of a dictionary attack, and make it much harder for an attacker to crack.

6.2.4 Access point Placement.

Placing the APs in areas so the signal does not propagate too far outside the confines of the office is advisable to minimise the area that an attacker can use to launch an attack.

6.2.5 Security Assessment

As discussed in section 5, a security assessment should be done, preferably by an external company. This has the effect of outlining security holes that can be fixed, and making us aware where we are vulnerable to attack so to make us better prepared for such an event. Such assessment should not be one off, but instead should be scheduled at least once a year, more often if security is a major factor on the network.

7.0 Ongoing Security Monitoring

7.1 Intrusion Detection Systems (IDS)

In this section we will look into all aspects of Intrusion Detection Systems including the different types of systems, how they work, how to deploy an IDS and a summary of the benefits of using IDS. Such systems are the final piece in the puzzle of deploying a secure network, be it wireless or not. By continually monitoring our network we can be made aware of any breaches as soon as they happen, allowing us to take preventative measures and if possible, close any holes discovered. It should always be kept in mind that a network once proved secure, is not always going to be so.

Particular attention will be paid in this section to how such systems can be specifically useful to improving WLAN security.

However first we can show how all types of IDSs adhere to an overall process model due to the fact that there are three essential components to all modern IDSs.

- *Information Sources* – An Intrusion can be detected through event information arising from a number of levels of a system. Network, Host and Application are by far the most popular sources of data for IDSs.
- *Analysis* – Data alone is not enough to detect an intrusion. How that data is analysed and made sense of is also vital to ensure a system can identify the signs of an Intrusion occurring or having occurred. The common techniques for analysis are misuse detection and anomaly detection.
- *Response* – After an intrusion has been identified an IDS must carry out some form of action. These measures are defined as being active or passive in their nature although a system can carry out both if required. A passive response would normally involve reporting the occurring events to a human administrator while an active response would comprise automated actions by the system.

7.1.1 Types of IDS

This section will look into the three main classifications of IDS: Host, Network and Application. They are named after their chosen information source. Although the common process model shows that there are also differences in IDSs Analysis and Response components the main criteria used to define an IDS is its Information Source, this highlights the importance of using the correct information to detect intrusions.

7.1.1.1 Host Based IDS

Host Based IDSs (HIDS) operate on individual computer systems using the base of information collected from within those individual computer systems. This placement allows them access to the most detailed information available in the form of specific files, system processes, registry settings and various log files.

The two main specific sources of information in a HIDS are the Operating system audit trails and system logs. Audit logs are created by the core of the operating system and are therefore highly detailed however this can mean they can be difficult to analyse. System logs on the other hand are much smaller and less complex to analyse and understand. A good HIDS will monitor a mixture of these sources to ensure the best possible coverage of the system in terms of accuracy, detail and timeliness.

These sources of information allow HIDS to analyse data with high levels of accuracy and reliability meaning they can often identify the specific accounts and processes involved in an attack on the operating system. HIDS also allow for “after action” reporting (Unless the HIDS has been disabled in the attack) as they directly monitor the files and system processes that will have been attacked.

A derivative of HIDS is centralized-host-based intrusion detection (CHIDS) that serves the same purpose but does the analysis centrally by sending monitored files, logs and registry settings to the manager for analysis. The primary differences between these systems are as follows.

- CHIDS is more secure because it sends all the needed information off the host so that if the host is compromised, the alerting and forensic analysis can still take place. The tradeoff is that centralized analysis requires substantially more network bandwidth to move the data to the manager.
- HIDS makes compliance decisions locally and only sends alerts to the manager when warranted. This uses substantially less network bandwidth. The shortcoming of HIDS is that if the host is compromised there is no alert or forensic data to determine what happened or what was lost.

Advantages:

- HIDS with their local information sources can detect attacks on their system that would go undetected by purely network based IDS.
- Can automatically replace altered files when changed to ensure data integrity.
- They can detect Trojan Horse or any other attack that involves altering the execution of software as HIDSs monitor the software processes and would recognize inconsistencies.

Disadvantages:

- HIDS entail a higher administrative workload due to the need to configure the systems on every host being monitored.

- Due to use of logs that only record events that have already occurred concern that HIDS are not “Real Time”.
- Due to the fact that HIDS are constantly monitoring files, logs and processes on the host there is a performance cost on the monitored system.
- Due to the fact that HIDS rely solely on local system information they could be targeted as part of an attack and disabled, leaving the host defenseless.
- HIDS often fail to notice network scans and other suspicious surveillance techniques due to the fact that they only know what packets their host has received.

7.1.1.2 Network Based IDS

Network Based IDSs (NIDS) form the bulk of IDSs in use today. These IDSs use the network wire as their information source as they capture and analyse network packets passing by them.

NIDS consist of one or more sensors or hosts, dedicated to monitoring packets, placed at various points around a network, often at pivotal points such as switches or routers. These sensors perform local analysis of the data collected from the wire, when an attack has been detected it is reported to a central management console elsewhere in the network. A single management console will cover multiple sensors over a LAN or even WAN.

This approach means a single sensor placed at the gateway switch or router to a network or sub-network can protect all hosts that lie behind it in the network topology. This is in contrast to the HIDS approach where only the machine the HIDS resides on is protected.

It is also possible for these sensors to be made “Stealthy” so that an attacker cannot discover their presence and location and thus launch a pre-emptive attack on them.

Some NIDS have refined their monitoring activities to look at the actual TCP/IP stack to ensure a better coverage of data passing over the wire. For example the ISS Real Secure Guard device creates a virtual TCP/IP stack where virtual versions of actual packets are interrogated. It contains a set of rules that “Good” TCP/IP packets adhere to and therefore “Bad” packets are likely to break some of these rules. These offending packets can then be blocked while all good packets will pass on unaffected.

Advantages:

- A few well-placed sensors can provide IDS coverage to a large number of hosts.
- They are relatively easy to deploy in an existing network environment as they are usually passive devices merely listening to traffic on the network

wire. An unprotected network can have NIDS added without major disruption or cost.

- As they act in a passive manner NIDS have a very small signature and thus are less likely to be detected by an attacker and attacked themselves. HIDS are more visible.
- NIDS can interact with other perimeter technologies to strengthen the network perimeter. NIDS leverages the existing investment in routing and firewall technologies by dynamically updating other perimeter policies to respond to threats in real-time. This can include adding a rule to a firewall to block traffic from a specific IP address stopping an attack as it occurs.

Disadvantages:

- NIDS struggle when the network load rises over 35% (Richard Barber, 2001) due to the fact that they cannot process and analyse all packets when they are being transmitted at those volumes. Purely hardware based solutions help to a degree as they remove some of the overheads of processing packets and can analyse more packets than a software solution. However if packets are not analysed this could mean an attack could be carried out and be missed by the NIDS.
- NIDS cannot analyse encrypted information, increasing use of VPNs means data will be passing the NIDS that it cannot check for signs of attack.
- Most NIDS are not very useful for indicating whether an attack they recognised was actually successful. HIDS have to be in operation for this information to be available.

7.1.1.3 Application Based IDS

Application based IDS are a special derivative of generic HIDS as they reside on a host to analyse events occurring within a specific software application, commonly a web or database server. As with HIDS they use transaction log and audit files as their information source. However, Application based IDSs use software rather than system logs.

Application based IDS are used to detect suspicious behaviour in companies most vital applications as they are tailored to analyse events within a single application with large amounts of application specific knowledge. The use of this knowledge would not be possible in HIDS or NIDS as they cover too much data. Application based IDS allow high quality analysis to occur at the vital point where the user and application interact and any attacks would be visible.

Advantages:

- Application based IDS can monitor the data exchange between users and the application. This is not possible with HIDS or NIDS. This allows them to trace unauthorised access back to a particular user.

- Application based IDS can also work with encrypted data, using application-based encryption/decryption services. This encrypted data would be unavailable for analysis on a wire monitored by a NIDS.

Disadvantages:

- Application based IDS are more vulnerable to attack than HIDS as they use application logs that are not as attack resistant as OS logs used by HIDS. If they were disabled the Application based IDS would be blind and an attacks could occur with impunity.
- As Application based IDS use the application logs they are unlikely to detect a software tampering attack, such as a Trojan Horse, as it would likely involve spoofing the contents of the logs.
- Application based IDS can also consume significant application (and host) resources.

7.1.2 How IDS Works

This section will look into the two other components of an IDS after the information source, Analysis and Response. As before there are different approaches that can be taken when considering the analysis of information and the response that is triggered when analysis indicates an attack is taking place. This section will look at each approach and consider its benefits and drawbacks.

7.1.2.1 IDS Analysis

This section will look at the two main forms of data analysis used by IDSs. Some IDSs primarily use a technique called signature detection while some use an approach called anomaly detection (also known as Heuristics). It appears that the most effective IDSs use mostly misuse detection methods in conjunction with a small number of anomaly detection components.

7.1.2.1.1 Misuse Detection

The by far most popular method of analysis for IDSs, Misuse Detection, involves looking for events or sets of events that match pre-defined patterns held in the IDSs attack signatures. The attack signatures are a database of traffic or activity patterns related to known attacks. This resembles the way many anti virus programs use virus signatures to recognize and block infected files and programs from entering a computer system, except that Misuse Detection uses a database of traffic or activity patterns related to known attacks instead. These signatures have to be regularly updated to ensure the system is aware of the latest patterns of attacks. Due to this

reliance on static signatures misuse detection is also called “Signature based detection”.

Advantages:

- Due to their high level of automation Misuse Detectors allow system administrators to quickly track security problems on their systems even if they themselves are not aware what the attack is they can initiate incident handling procedures.
- They can quickly and reliably diagnose what attack tool or technique is being used, this can speed up the use of the correct corrective measure for that attack.
- Misuse Detection works well detecting attacks without generating an overwhelming number of false alarms. Unless entirely new attacks are being carried out, as this is Misuse Detections Achilles heel.

Disadvantages:

- Misuse Detection requires the attack signatures to be constantly updated otherwise attacks will occur that they have no knowledge of and therefore will take no action against.
- To reduce the number of false positives (Alarms when there is no attack) Misuse Detection uses very tightly defined signatures. However this means they will miss variants of existing attacks, as this is the most common way of creating a new attack this is a problem.
- Signature-based IDSs can also impose noticeable performance drags on systems when current behaviour matches multiple attack signatures, either in whole or in part.

7.1.2.1.2 Anomaly Detection

Anomaly detection involves identifying abnormal behaviour in the data being analysed. This whole form of detection is predicated on the assumption that attacks take the form of activity different from “normal” activity and therefore can be detected if the system looks for “abnormal” activity.

For an anomaly detection to function the normal level and form of activity must be discovered. This can involve measuring a "baseline" of such stats as CPU utilization, disk activity, user logins, file activity, and so forth. This baseline is constructed from data collected over a period of time encompassing normal network/host activity. The system then collects event data and uses a variety of measures to determine when there is a deviation from this baseline; at this point the usual response can be triggered.

There are a variety of techniques being researched and used in anomaly detection they include:

- Threshold detection involves certain critical attributes being given values and those values being monitored with a target value at which an alarm would be triggered if the count reaches it. For example an alarm may be raised if there were more than 4 failed logins on a single host in a 24-hour period. These thresholds can be static or heuristic. Heuristic involves changing the target value to reflect changes in the average value for that attribute over time. This aims to reduce false positive numbers.
- Statistical Measures looks attributes over time and deduces patterns from them. Activity that strays too far from the expected pattern is then assumed to be an attack.
- Research continues into other innovative approaches including neural networks, genetic algorithms and models based on the human immune system.

Currently only threshold detection and statistical measures are used in any commercial IDSs.

Advantages:

- By creating baselines of normal behaviour, anomaly-based IDSs can observe when current behaviour deviates statistically from the norm. This capability theoretically gives anomaly-based IDSs abilities to detect new attacks that are neither known nor for which signatures have been created.
- Can be used to produce information that can be used in conventional misuse detection systems.

Disadvantages:

- Normal behaviour can change easily and readily therefore anomaly-based IDSs are prone to false positives where attacks may be reported based on changes to the norm that are “normal,” rather than representing real attacks
- The necessity, difficulty and time taken to train the system to understand the normal noise and behaviour of its information source can be off-putting compared to the almost “Plug and Play” nature of misuse detection.
- Anomaly detections intensely analytical behaviour can also impose heavy processing overheads on systems where they’re running.

7.1.2.2 IDS Responses

The final stage in the generic IDS process model after information has been collected and analysed is that of the response the IDS will generate to a perceived attack.

The responses an IDS can make are broadly described as Active or Passive, these can be carried out in isolation or concurrently.

7.1.2.2.1 Active Responses

Active responses are automated actions that an IDS performs when an intrusion is detected. Different intrusions elicit different responses. There are three main categories of active responses:

Collect Additional Information

The most immediate concern of an IDS when it believes it has detected an intrusion is to try and confirm that suspicion by searching for more information. Although this is a fairly benign action it often is the most important as more information about the intrusion can help defend against it or show it to be a false positive alert, both of these outcomes are desirable.

Examples of actions taken to learn more include increasing the sensitivity of the IDS so that it takes a more detailed look at the events occurring. As well as obviously providing more detail for the analysis engine of the IDs it can also turn out to be useful if an attack does occur and evidence of the events is required. This can involve saving the raw packets to allow independent verification of the activity that occurred.

Change the Environment

A more proactive response and one wanted by most network administrators are to attempt to stop an intrusion as it happens and block subsequent attempts by the attacker. The basic action is to identify the source IP address of the attack and block packets from that address. This is not done by the IDS but by the firewall. The IDS sends a message to the firewall instructing it to create a new "Block" rule for the attackers IP address. Other options for the IDS to reconfigure are to block network ports, protocols or services being used on the target machine. A worst case scenario option is to reconfigure routers and firewalls to sever all connections on the network interface the attack is being carried out over.

Take Action Against the Intruder

Most IDSs utilise the first two forms of active response, however there is a third far more offence minded and controversial method, a strike back attack on the attacker.

This is however considered a very bad idea for a number of reasons. Firstly it may cause the incident to escalate and incur even more attacks on your system from an angry hacker or group of hackers. Secondly due to the use of spoofed addresses by attackers the likelihood of a strike back at an innocent computer system or network is very high. Finally the legal issues are very vague and if discovered the instigator of a strike back may be considered an attacker themselves, with all the legal implications this entails.

Overall IDS systems are purely defensive measures and unless there is a change in law and technology are likely to remain just that.

7.1.2.2.2 Passive Responses

In contrast to the automated active responses an IDS can make passive responses rely on humans to take action after the alarm has been raised. Some basic IDSs may provide for passive responses only.

Most commercial IDSs allow users to select from many options for passive responses to a detected intrusion. They can select a single response or a collection of responses to ensure the system administrators are aware of the threat and take the correct action.

The most common form of alert is an onscreen popup box showing the details of the suspected intrusion. The user can define what level of detail they want to be displayed in these messages from a simple “You are under attack!” to ones including the suspected source IP and tools used by the attacker. This visual message may be set to appear on a server or on the system administrators own workstation. These visual messages can also be accompanied by a WAV file being played, possibly an alarm noise or recorded “You are under attack!” message.

For large organisations the ability to send messages via mobile communication channels is also very useful. The classic example is of an IDS sending a message to the system administrators pager, however nowadays a text message sent to their mobile phone is the more likely choice.

Finally SNMP traps can be used to send a message to a central network management console allowing the network support staff to take action even if they are not based at the actual location of the target of the attack.

7.1.2.3 IDS Reporting

The main function of an IDS is to detect and then assist in the prevention of intrusions into a computer system or network. However it is also useful if they can be used to asses long-term trends in attacks and allow an organisation to use this information to help improve their defences and spend their budgets in the most effective way. Therefore many IDSs contain reporting functions that collate and display information about attacks and activity in a variety of ways for analysis and decision-making uses. This can allow an organisation to asses trends over a variety of time periods, e.g. last week, month or year etc, to improve and alter their system security set-up to suit the needs of that particular organisation.

7.1.3 Deployment of IDS

After an organisation has decided to deploy an IDS system they must then decide where to place it within their network topology. NIDSs can be placed in a variety of locations with differing advantages while HIDSs also have options for deployment that need to be considered.

The diagram below (Figure 5) shows an example of an IDS protected network with the variety of possible deployment options. This also illustrates how the options are not exclusive and that, if required, IDS systems can be deployed across a network at various points. This would provide far more comprehensive and accurate coverage than a single point system, however the cost will be far greater.

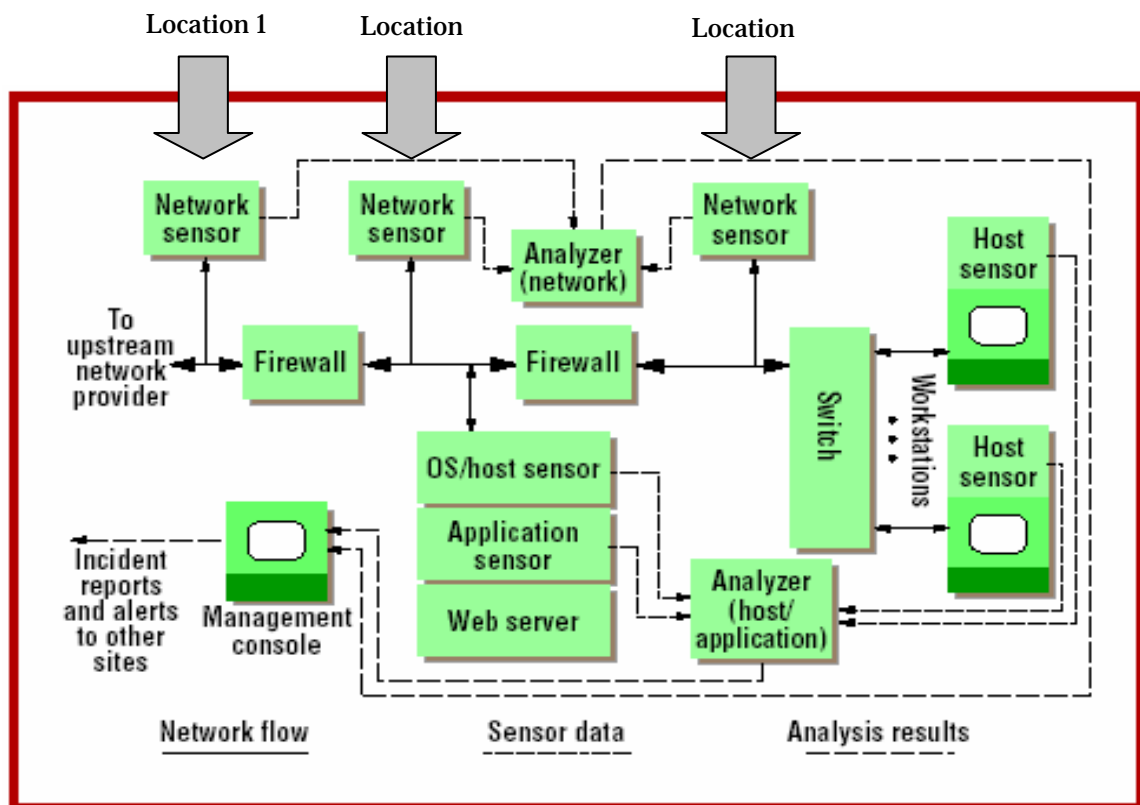


Figure 5: An IDS protected enterprise from IEEE Software September/October 2000

NIDS Deployment

See Figure 5 For Locations

Location 1: Beyond the outer firewall

This location is of most use to a large organisation that wants to see and document the number and type of attacks that are launched against the network from the Internet. It is hoped many of these will be blocked by rules enforced by the outer firewall.

Location 2: Behind outer firewall in DMZ

A NIDS in this location will detect attacks that have breached the outer firewalls rule set; as this is documented the system administrators can assess the firewalls performance and use the information to improve its policies to stop more attacks in future. This location can also notice outward traffic from a compromised server and ensure the appropriate actions are taken.

Location 3: On network backbone

As an IDS system on the network backbone will monitor much greater levels of traffic than elsewhere it is more likely that it will detect attacks taking place. Also this location allows the system to check for unauthorised activity carried out by users within the network itself.

HIDS Deployment

Due to the large number of hosts in a large network deploying HIDS on every one is unfeasible, costly and extremely time consuming. Therefore it is far more efficient to select the most vital hosts on a network and deploy HIDS on these systems only.

By far the most important single nodes on any network are the servers. Often this will include a number of file, application, database, web and ftp servers. With these critical nodes protected by HIDS a network is very well protected.

It is also possible that HIDS may be run on a small number of client workstations if they are considered important enough. The CEO, all Directors and perhaps R&D PC's where cutting edge work is carried out would be likely high value nodes that deserve protection from HIDS.

7.1.4 Commercially Available IDSs

This section will show a range of available IDSs in the commercial marketplace; this is in addition to the many freely available products. For enterprise level security only commercial solutions would be considered.

Cisco Secure IDS (formerly NetRanger)		
Hardware	Cisco Systems	http://www.wheelgroup.com/warp/public/cc/pd/sqsw/sqidsz/index.shtml
Network-based, misuse detection. An enterprise-scale, real-time, intrusion detection system designed to detect, report, and terminate unauthorized activity throughout a network. When NetRanger analyses network data, it looks for patterns of misuse.		
Cyclops		
Both	e-Cop.net	http://www.e-Cop.net
Snort-based Cyclops IDS provides advanced and flexible intrusion detection at Gigabit speeds and secures networks by performing high-speed packet analysis to detect malicious activities in real-time and automatically launch preventive measures before security can be compromised		
E-Trust IDS		
Software	Computer Associates	http://www3.ca.com/Solutions/Product.asp?ID=163
eTrust Intrusion Detection delivers state-of-the-art network protection including but not limited to, defence against deployment and execution of Distributed Denial of Service (DDOS) attacks, malicious and unauthorized use of internet facilities and other network misuse events.		
Manhunt		
Both	Symantec	http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=156
Symantec ManHunt provides high-speed, network intrusion detection, real-time analysis and correlation, and proactive prevention and response to protect enterprise networks against internal and external intrusions and denial-of-service attacks.		
NFR Sentivist		
Both	NFR Security	http://www.nfr.com/solutions/system.php
With NFR Security's intelligent intrusion management system, you'll not only detect and deter network attacks; you also integrate with popular firewall providers to prevent future attacks.		
RealSecure Network Sensor		
Both	ISS	www.iss.net/products_services/enterprise_protection/rsnetwork/sensor.php
The RealSecure Network Sensor provides broad-based detection, prevention and response for attacks and misuse that originate from across a network. Automatic responses to improper activity include log events to a database, block a connection, send an email, suspend an account, disable an account, or create a user defined alert.		
SecurityMetrics		
Hardware	SecurityMetrics	http://www.securitymetrics.com/securitymetricsappliance.adp
Once connected to your network the Security Appliance begins sensing all network traffic. It looks at each packet travelling across the network and determines if the packets are safe or if they are attacks to your network. The SecurityMetrics Appliance will notify you in real-time whenever an attack occurs on your network.		

Wireless IDS

However in addition to the established forms of IDS there is also a new form of IDS system specifically developed for WLANs and utilising WLAN technology. The leading AirDefense Guard product best displays wireless IDS (WIDS) in action.

AirDefense Guard consists of distributed wireless sensors and server appliances. The remote sensors sit near 802.11a/b/g access points to monitor all WLAN activities and report back to the server appliance, which analyses the traffic in real time. This means AirDefense guard can detect attacks as they occur as it is constantly monitoring and analysing the actual RF emissions in its area.

The figure below (Figure 6) shows how the remote sensors and the central hardware appliance work together to detect threats to the wireless network.

This is a much more proactive approach to WLAN security than traditional IDS and is a useful addition to the armory of the Network Security Manager.

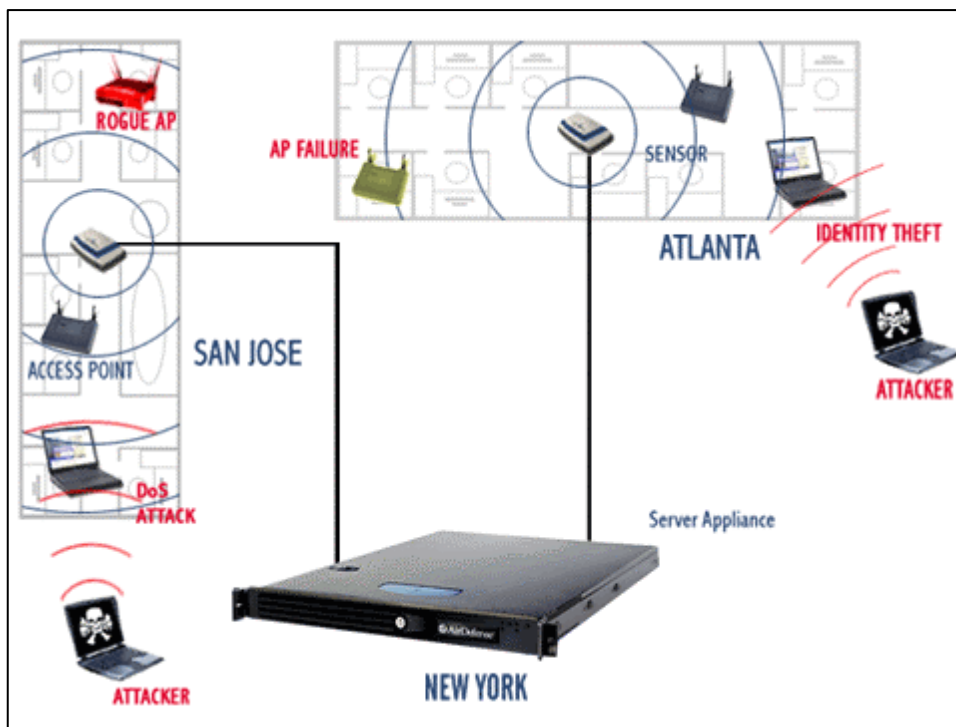


Figure 6: AirDefense Guard in operation from www.airdefense.net/products/airdefense_ids.shtm

8.0 Conclusions and Critical Evaluation

The aims of this project were to investigate the areas of wireless security assessment and continuous security monitoring using Intrusion Detection Systems (IDS); this involved defining the concept of security in general, wireless security and Intrusion Detection.

We found that the areas investigated were quite clearly defined with obvious subjects that could be investigated.

The sections of the report included Security assessment using the latest techniques and this required a large amount of background reading around the subject, before investigating the specifics of Wireless Auditing.

The report also included a section on continuous security monitoring utilising IDS which involved a large amount of theoretical research. By furthering our knowledge of IDS we were also able to construct a small practical tutorial which could be used by students interested in this area.

As a group we feel that we had enough time to fully investigate and understand the topics covered in the project, therefore we feel that the theoretical component of the project is of a good quality. In contrast, due to constraints on equipment and time, we were unable to carry out any practical experiments relating to auditing a wireless network. The lack of a practical element caused disappointment in the group as it meant the project was then almost completely theoretical, with no practical work to back up its recommendations and findings.

The academic work covered in this report is of a very good quality as we all researched from a large and diverse range of sources and then peer-reviewed each others work to ensure a high level of consistency and standard.

The project could easily be developed by adding a practical element, investigating the realities of carrying out a wireless security audit. The findings from a practical section would provide solid, first hand experience of this subject area. The knowledge gained, could therefore help to refine the material in our project.

9.0 References & Bibliography

9.1 References

Davies, J (2003) *Deploying Secure 802.11 Wireless Networks with Microsoft Windows*, Microsoft Press

Edney, J and Arbaugh, W (2004). *Real 802.11 Security - Wi-Fi Protected Access and 802.11i*, Addison-Wesley

Heady, R et al. (1990) *The architecture of a network level intrusion detection system*, Technical Report CS90-20, University of New Mexico, Department of Computer Science, August 1990

McHugh, J et al. (2000) *Defending Yourself: The Role of Intrusion Detection Systems*, IEEE Software, September/October 2000

Online Staff (2003) *Intrusion Prevention \$924m Market By 2006*, Computergram Weekly; 12/5/2003 Issue 4814, p10, [Internet]
<http://search.epnet.com/direct.asp?an=11611561&db=buh> [Accessed 15.02.04]

Potter, B and Fleck, B (2002) *802.11 Security*, O'REILLY

9.2 Bibliography

Airdefense (2003) *Wireless LAN Policies for Security and Management* [Internet]
http://www.airdefense.net/whitepapers/paper_policy.shtm [Accessed 05.02.04]

Bace, R and Mell, P (2001) *Intrusion Detection Systems*, NIST Special Publication 800-31 [Internet] <http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf> [Accessed 10.02.04]

Barber, R (2001) *The Evolution of Intrusion Detection Systems — The Next Step*, Computers & Security, **Vol. 20**, No. 2, pp. 132-145

Baumann, R and Plattner, C (2002) *Honeypots*, Swiss Federal Institute of Technology Zurich

Bierman, E et al. (2001) *A Comparison of Intrusion Detection Systems*, Computers & Security, **Vol. 20**, No. 8, pp. 676-683

Dobrotka, D (2003) *Intrusion detection on a Wireless Network?* [Internet] http://www.sans.org/resources/idfaq/wireless_ids.php [Accessed 10.02.04]

Geier, J (2002) *Wireless LAN Security Assessments Steps* [Internet] <http://www.wi-fiplanet.com/tutorials/article.php/1545731> [Accessed 05.02.04]

Graham, R (2000) *FAQ: Network Intrusion Detection Systems* [Internet] <http://www.ticm.com/kb/faq/idsfaq.html> [Accessed 10.02.04]

Halme, L and Bauer, R (2003) *A Taxonomy of Anti-Intrusion Techniques* [Internet] <http://www.sans.org/resources/idfaq/aint.php> [Accessed 10.02.04]

Heath, A (2002) *Investigation into wireless networking technologies and evaluation of current security aspects*,
School of Computing and Management sciences, Sheffield Hallam University

International Network Services (2003) *Wireless Security Assessment* [Internet] http://www.ins.com/downloads/datasheets/ngn_wireless_secassessment_ds_emea.pdf [Accessed 05.02.04]

Internet Security Systems (2001) *Wireless LAN Security* [Internet] http://www.thc.org/misc/docs/802.11/10_wireless_LAN_security.pdf [Accessed 05.02.04]

Karygiannis, T and Owens, L (2002) *Wireless Network Security*, NIST Special Publication 800-48 [Internet] http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf [Accessed 05.02.04]

Kerschbaum, F et al. (2002) *Using Internal Sensors and Embedded detectors for Intrusion Detection*, Journal of Computer Security, **Vol. 10**, No. 1, pp.23-70

Kuehl, K (2000) *Detecting Rogue 802.11 Access Points Within the Enterprise* [Internet] <http://winfingerprint.sourceforge.net/presentations/APTools.ppt> [Accessed 06.02.04]

Kurtz, G and Prosize, C (2000) *Penetration Testing Exposed* [Internet] <http://infosecuritymag.techtarget.com/articles/september00/features3.shtml> [Accessed 06.02.04]

Magalhaes, R (2003) *Host-Based IDS vs. Network-Based IDS* [Internet] http://www.windowsecurity.com/articles/Hids_vs_Nids_Part1.html [Accessed 10.02.04]

Ollmann, G (2003) *Securing WLANTechnologies* [Internet]

<http://www.technicalinfo.net/papers/SecuringWLANTechnologies.html> [Accessed 05.02.04]

Saarinen, H (2002) *Analysis and Implementation of the Wireless Local Area Network (IEEE802.11B) standard within a corporate environment*, School of Computing and Management Sciences, Sheffield Hallam University

Spitzner, L (2002) *Honeypots: Tracking Hackers*, Addison Wesley

Sundaram, A (2001) *An Introduction to Intrusion Detection* [Internet]

<http://www.acm.org/crossroads/xrds2-4/intrus.html> [Accessed 10.02.04]

Verwoerd, T and Hunt, R (2002) *Intrusion Detection Techniques and Approaches*, Computer Communications, **Vol. 25**, Issue 15, pp. 1356-1365, [Internet]

<http://www.sciencedirect.com/science/article/B6TYP-45RFC2C-2/2/5245aa91a2efdfa8130bb42d93bea6e8> [Accessed 10.02.04]

Wack, J et al. (2003) *Guideline on Network Security Testing*, NIST Special Publication 800-42 [Internet] <http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf> [Accessed 05.02.04]

Wi-Fi Alliance (2003) *Wi-Fi Protected Access:*

Strong, standards-based, interoperable security for today's Wi-Fi networks

[Internet] http://www.weca.net/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf [Accessed 05.02.04]

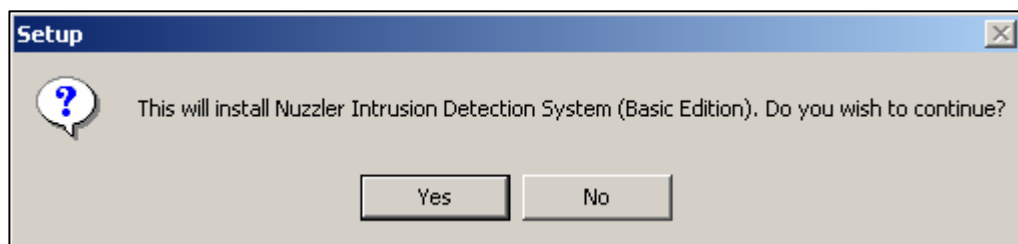
Appendices

Appendix 1 IDS Practical Tutorial

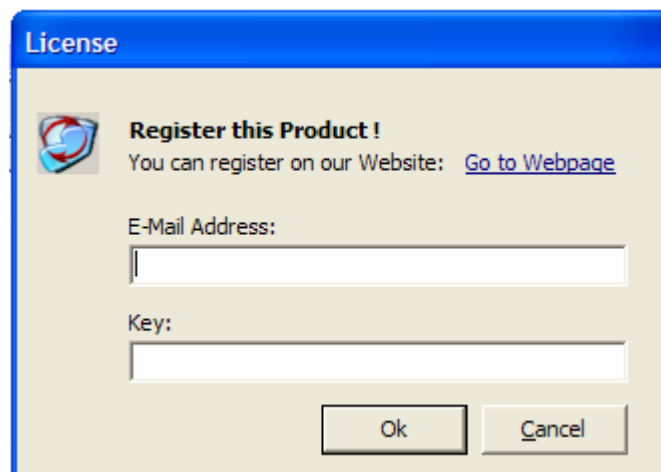
Intrusion Detection Tutorial

How to get a basic Intrusion Detection System running on your PC.

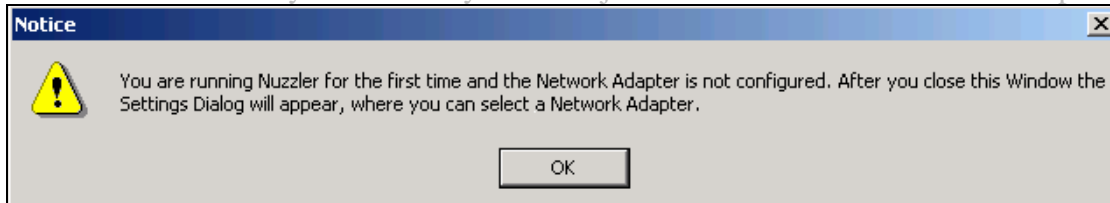
1. Download the Shareware version of SecurePoint IDS from <http://download.com.com/3000-2092-10162205.html?tag=lst-0-1>
2. Double Click on the downloaded .exe file.
3. Click Yes to start the installation process.



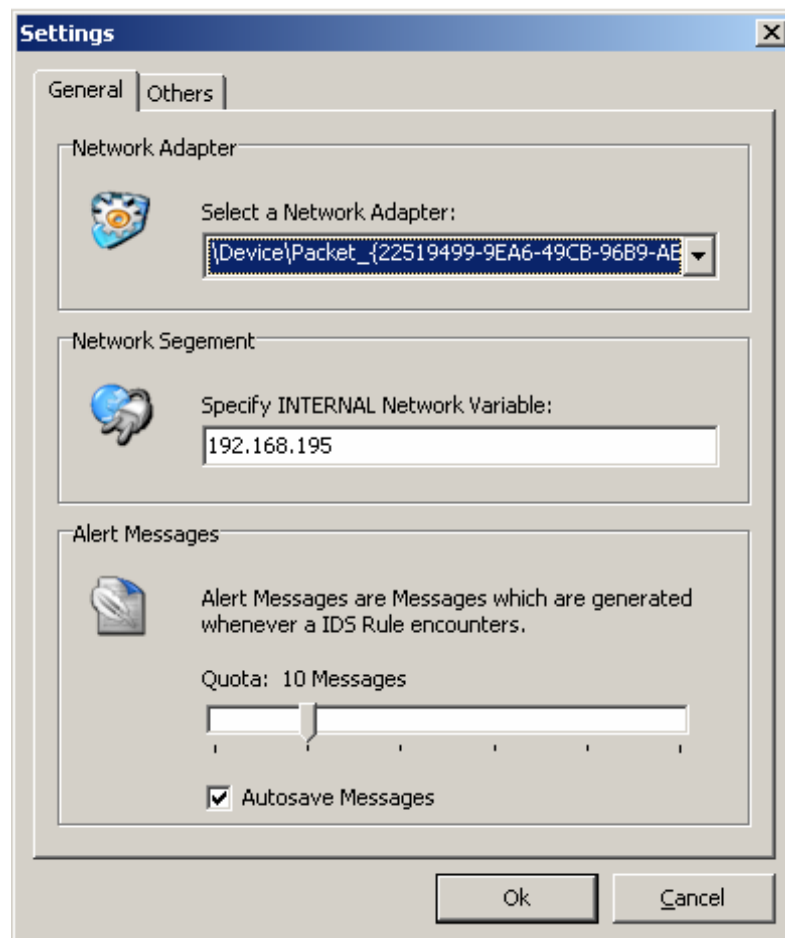
4. Go through the normal installation procedure, accepting default values throughout.
5. After installation is complete restart PC as requested.
6. When you start SecurePoint IDS you are required to register to get the key required for operation of the software. Click the link "Go to Webpage", fill out the form and enter the registration key you receive in the dialogue box shown below.



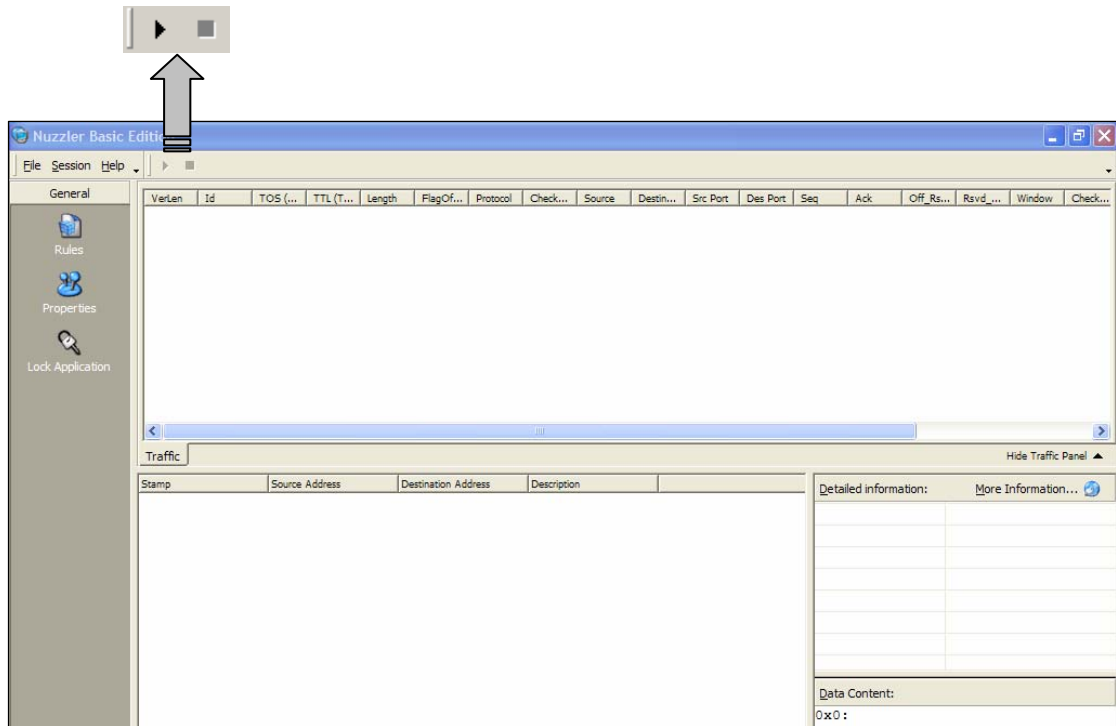
7. You now have a functional copy of SecurePoint IDS running on your system. You will immediately see the following message appear on your screen. Select OK to proceed.



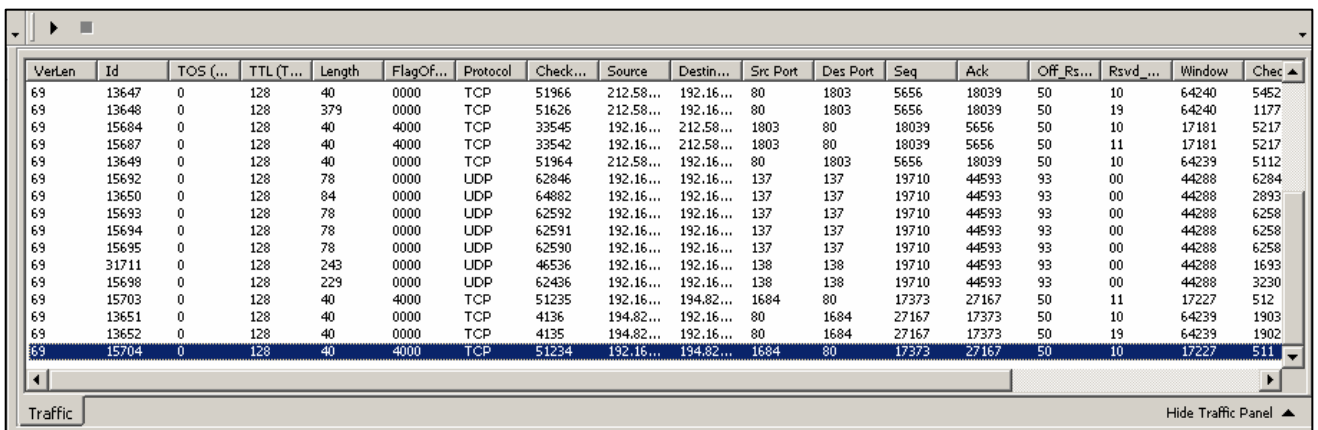
8. You will then see the display below. You first need to select the Network Adaptor you want to monitor and then enter your network IP address (Your PC's IP address without the host part).



10. The SecurePoint IDS system is now properly set-up. Click the Run button to start the system (Shown Below)



11. Any packets sent via the selected Network Adaptor will now be logged in the SecurePoint IDSs main window. Their type, source, destination, content etc are all recorded. This is shown below



12. From now on any traffic that contravenes SecurePoint's many rules will be flagged up as an alert. This will allow you to look at the offending packets and decide if an intrusion is taking place. This will allow you to take any necessary action, e.g. Change Firewall settings, shut down Internet access.

Appendix 2 WLAN Security checklist

No.	Security Recommendation	Checklist		
		Best Practice	Should Consider	Status
Management Recommendations				
1.	Develop an agency security policy that addresses the use of wireless technology, including 802.11	yes		
2.	Ensure that the users on the network are fully trained in computer security awareness and the risks associated with wireless technology.	yes		
3.	Perform a risk assessment to understand the value of the assets in the agency that need protection.	yes		
4.	Ensure that the client NIC and AP support firmware upgrade so that security patches may be deployed as they become available (prior o purchase).	yes		
5.	Perform comprehensive security assessments at regular and random intervals (including validating that rogue APs do not exist in the 802.11 WLAN) to fully understand the wireless network security posture.	yes		
6.	Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.	yes		
7.	Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).	yes		
8.	Complete a site survey to measure and establish the AP coverage for the agency.	yes		
9.	Take a complete inventory of all APs and 802.11 wireless devices.	yes		
10.	Ensure that wireless networks are not used until they comply with the agency's security policy.	yes		
11.	Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.	yes		
12.	Place APs in secured areas to prevent unauthorized physical access and user manipulation.	yes		
Technical Recommendations				
13.	Empirically test AP range boundaries to determine the precise extent of the wireless coverage.	yes		
14.	Make sure that APs are turned off during when they are not used (e.g., after hours and on weekends).	yes		
15.	Make sure that the reset function on APs is being used only when needed and is only invoked by an authorized group of people	yes		
16.	Restore the APs to the latest security settings when the reset functions are used.	yes		
17.	Change the default SSID in the APs.	yes		
18.	Disable the broadcast SSID feature so that the client SSID must match that of the AP		yes	

19.	Validate that the SSID character string does not reflect the agency's name (division, department, street, etc.) or products.	yes		
20.	Ensure that AP channels are at least five channels different from any other nearby wireless networks to prevent interference	yes		
21.	Understand and make sure that all default parameters are changed.	yes		
22.	Disable all insecure and nonessential management protocols on the APs.	yes		
23.	Enable all security features of the WLAN product, including the cryptographic authentication and WEP privacy feature.	yes		
24.	Ensure that encryption key sizes are at least 128-bits or as large as possible.	yes		
25.	Make sure that default shared keys are periodically replaced by more secure unique keys.	yes		
26.	Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to APs).	yes		
27.	Install antivirus software on all wireless clients.	yes		
28.	Install personal firewall software on all wireless clients.	yes		
29.	Disable file sharing on wireless clients (especially in untrusted environments).	yes		
30.	Deploy MAC access control lists.		yes	
31.	Consider installation of Layer 2 switches in lieu of hubs for AP connectivity.	yes		
32.	Deploy IPsec-based Virtual Private Network (VPN) technology for wireless communications.		yes	
33.	Ensure that encryption being used is sufficient given the sensitivity of the data on the network and the processor speeds of the computers.	yes		
34.	Fully test and deploy software patches and upgrades on a regular basis.	yes		
35.	Ensure that all APs have strong administrative passwords.	yes		
36.	Ensure that all passwords are being changed regularly.	yes		
37.	Deploy user authentication such as biometrics, smart cards, two-factor authentication, and PKI.		yes	
38.	Ensure that the "ad hoc mode" for 802.11 has been disabled unless the environment is such that the risk is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor	yes		
39.	Use static IP addressing on the network		yes	
40.	Disable DHCP.		yes	
41.	Enable user authentication mechanisms for the management interfaces of the AP.	yes		
42.	Ensure that management traffic destined for APs is on a dedicated wired subnet.	yes		
43.	Use SNMPv3 and/or SSL/TLS for Web-based management of APs.	yes		
Operational Recommendations				
44.	Configure SNMP settings on APs for least privilege (i.e., read only). Disable SNMP if it is not used. SNMPv1 and SNMPv2 are not recommended.	yes		
45.	Enhance AP management traffic security by using SNMPv3 or equivalent cryptographically protected	yes		

	protocol.			
46.	Use a local serial port interface for AP configuration to minimize the exposure of sensitive management information.		yes	
47.	Consider other forms of authentication for the wireless network such as RADIUS and Kerberos		yes	
48.	Deploy intrusion detection agents on the wireless part of the network to detect suspicious behaviour or unauthorized access and activity.		yes	
49.	Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity.		yes	
50.	Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features.		yes	
51.	Enable utilization of key-mapping keys (802.1X) rather than default keys so that sessions use distinct WEP keys.	yes		
52.	Fully understand the impacts of deploying any security feature or product prior to deployment	yes		
53.	Designate an individual to track the progress of 802.11 security products and standards (IETF, IEEE, etc.) and the threats and vulnerabilities with the technology.		yes	
54.	Wait until future releases of 802.11 WLAN technologies incorporate fixes to the security features or provide enhanced security features.		yes	
55.	When disposing access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc	yes		
56.	If the access point supports logging, turn it on and review the logs on a regular basis.	yes		

Appendix 3 WLAN Security Summary

Security Recommendation		Security Needs, Requirements, or Justification
1.	Develop an agency security policy that addresses the use of wireless technology, including 802.11.	A security policy is the foundation on which other countermeasures—the operational and technical ones—are rationalized and implemented. A documented security policy allows an organization to define acceptable architecture, implementation, and uses for 802.11 wireless technologies.
2.	Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology (e.g., 802.11).	A security awareness program helps users to establish good security practices to prevent inadvertent or malicious intrusions into an organization's information systems.
3.	Perform a risk assessment to understand the value of the assets in the agency that need protection.	Understanding the value of organizational assets and the level of protection required is likely to enable more cost-effective wireless solutions that provide an appropriate level of security.
4.	Ensure that the client NIC and AP support firmware upgrades so that security patches may be deployed as they become available (prior to purchase).	Wireless products should support upgrade and patching of firmware to be able to take advantage of wireless security enhancements and fixes.
5.	Perform comprehensive security assessments at regular and random intervals (including validating that rogue APs do not exist in the 802.11 WLAN) to fully understand the wireless network security posture.	Security assessments, or audits, are an essential tool for checking the security posture of a WLAN and for determining corrective action to make sure it stays secure. Random checks ensure that the security posture is maintained beyond periods of assessment.
6.	Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.	The external boundaries should be secured to prevent malicious physical access to an organization's information system infrastructure such as a fence or locked doors.
7.	Deploy physical access controls to the building and other secure areas (e.g., using photo IDs or card badge readers).	Identification badges or physical access cards help to ensure that only authorized personnel have access to gain entry to a facility.
8.	Complete a site survey to measure and establish the AP coverage for the agency.	Proper placement of Access Points will help ensure that there is adequate wireless coverage of the environment while minimizing exposure to external attack. The site survey should result in a report that proposes AP locations, determines coverage areas, and assigns radio channels to each AP and that ensures that the coverage range does not expose APs to potential malicious activities.
9.	Take a complete inventory of all APs and 802.11 wireless devices.	A complete inventory list of APs and 802.11 wireless devices can be referenced when conducting an audit for unauthorized use of wireless technologies.
10.	Ensure that wireless networks are not used until they comply with the agency's security policy.	Security policy enforcement is vital for ensuring that only authorized APs and 802.11 wireless devices are operating in compliance with the organization's wireless security policy.
11.	Locate APs on the interior of buildings instead of near exterior walls and windows.	Locating APs near exterior walls and windows provides a better range of access to potential external malicious users. Choosing the location wisely to balance security and coverage should be considered.
12.	Place APs in secured areas to prevent unauthorized physical access and user	Physically securing the APs, putting them "out of reach," prevents unauthorized access

	manipulation.	by potential malicious users.
13.	Empirically test AP range boundaries to determine the precise extent of the wireless coverage.	By empirically testing the AP coverage range for an agency, a level of risk associated with the access range by potential malicious users can be better understood.
14.	Make sure that APs are turned off while they are not being used (e.g., after hours, weekends).	Shutting down APs when not in use minimizes potential exposure to malicious activity.
15.	Make sure that the reset function on APs is being used only when needed and is only invoked by an authorized group of people.	The reset function allows an individual to negate any security settings administrators have configured on an access point.
16.	Restore the APs to the latest security settings when the reset functions are used.	Security settings are lost after a reset function. Therefore, the appropriate personnel should restore the latest security settings after a reset.
17.	Change the default SSID in the APs.	Many default SSIDs used by vendors are published and well known. Malicious users often try to connect to 802.11 networks using the default SSID.
18.	Disable the broadcast SSID feature so that the client SSID must match that of the AP.	Malicious users can more easily detect and exploit APs that are broadcasting the SSID. Disabling the broadcast SSID feature minimizes exposure of the AP to malicious users
19.	Validate that the SSID character string does not reflect the agency's name (division, department, street, etc.) or products.	The SSID should be somewhat difficult for malicious users to use to determine the organization or agency that owns the AP. The SSID should also be long and difficult to guess.
20.	Ensure that AP channels are at least five channels different from any other nearby wireless networks to prevent interference.	Radio interference between APs can result in a denial of service. So, using channels in a different range ensures service availability.
21.	Understand and make sure that all default parameters are changed.	Because default settings are generally known and not secure, these settings should be changed and should comply with organizational security policy.
22.	Disable all insecure and nonessential management protocols on the APs.	Management protocols that are enabled on APs but not used present a potential avenue of attack. Disabling all insecure and nonessential management protocols minimizes potential methods that a hostile entity can use when attempting to compromise an access point.
23.	Enable all security features of the WLAN product, including the cryptographic authentication and WEP privacy features.	Enabling built-in security features provides greater security than the default settings.
24.	Ensure that encryption key sizes are at least 128 bits or as large as possible.	Brute force attacks on encryption key sizes become more difficult as the key sizes increase. The addition of a single bit doubles the key space. A 128-bit provides an "intractable" key space against cryptanalysis, if the algorithm and implementation are sound.
25.	Make sure that default shared keys are periodically replaced by more secure unique keys.	Changing default shared keys periodically decreases the likelihood that a malicious user can exploit a compromised key. A changed key increases the adversary's difficulty.
26.	Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to APs).	A firewall can enforce a security policy on the information flow between the wired network and the wireless network.
27.	Install antivirus software on all wireless clients.	Antivirus software helps ensure that the wireless client does not introduce known worms and viruses to the wired network while protecting the wireless client from viruses that originate on the wired network.
28.	Install personal firewall software on all wireless clients.	Personal firewalls help to protect against wireless network attacks.

29.	Disable file sharing on wireless clients (especially in untrusted environments).	Malicious users can potentially exploit wireless clients enabled for file sharing.
30.	Deploy MAC access control lists.	The use of access control lists based on MAC hardware addresses provides a layer of security that ensures that only authorized wireless devices are allowed to connect to the wired network.
31.	Consider installation of Layer 2 switches in lieu of hubs for AP connectivity.	The use of layer 2 switches segments network traffic and minimizes potential for a hostile user to monitor traffic by connecting to a hub.
32.	Deploy IPsec-based Virtual Private Network (VPN) technology for wireless communications.	The use of IPsec-based VPN provides an overlay protection to the standard link encryption (e.g., WEP) provided by the wireless connecting hosts.
33.	Ensure that encryption being used is sufficient with the sensitivity of the data on the network and the processor speeds of the computers.	Sensitive data transmission should be encrypted. The level of encryption provided must be balanced between data security requirement and overhead cost related to processor capability.
34.	Fully test and deploy software patches and upgrades regularly.	Newly discovered security vulnerabilities of vendor products should be patched to prevent malicious and inadvertent exploits. Patches should also be fully tested before implementation to ensure that they work.
35.	Ensure that all APs have strong administrative passwords.	Administrator passwords on APs should not be easy to guess. This minimizes the risk of an unauthorized user gaining access by guessing or cracking administrative passwords.
36.	Ensure that all passwords are being changed regularly.	Passwords should changed regularly to reduce the risk of a compromised password being exploited.
37.	Deploy user authentication such as biometrics, smart cards, two-factor authentication, or PKI.	Implementing strong or two-factor authentication whenever possible minimizes the vulnerabilities associated with simple username and password authentication.
38.	Ensure that the "ad hoc mode" for 802.11 has been disabled unless the environment is such that the risk is tolerable. Note: some products do not allow disabling this feature; use with caution or use a different vendor.	The "ad hoc mode" for 802.11 can be exploited. Users of hosts with "ad hoc mode" enabled may unintentionally allow users to inadvertently or maliciously connect to those systems.
39.	Use static IP addressing on the network.	Using static IP addressing makes it more difficult for a hostile user to connect to the network.
40.	Disable DHCP.	If DHCP is disabled, then hosts are forced to use a static IP address.
41.	Enable user authentication mechanisms for the management interfaces of the AP.	User authentication mechanisms should be enabled to ensure that only authenticated users are allowed access to the management interfaces of an AP.
42.	Ensure that management traffic that is destined for APs is on a dedicated wired subnet.	Passing management traffic over an "out of band" network or management subnet protects management traffic, interfaces, and passwords from organizational and outside users.
43.	Use SNMPv3 and/or SSL/TLS for Web-based management of APs.	SNMPv3 has enhanced security features relative to its predecessor SNMP protocol. SNMPv3 and SSL/TLS provide for secure authentication and encryption for Web-based management access of APs.
44.	Configure SNMP settings on APs for least privilege (i.e., read only). Disable SNMP if it is not used. SNMPv1 and SNMPv2 are not recommended.	Agencies that require SNMP should change the default community string, as often as needed, to a strong community string. Privileges should be set to "read only" if that is the only access a user requires. SNMPv1 and SNMPv2 message wrappers support only trivial authentication based on plain-text community strings and so are fundamentally insecure and not recommended. Agencies

		should use SNMPv3.
45.	Enhance AP management traffic security by using SNMPv3 or equivalent cryptographically protected protocol.	AP management traffic should be cryptographically protected. SNMPv3 provides cryptographic mechanisms to provide strong security.
46.	Use a local serial port interface for AP configuration to minimize the exposure of sensitive management information.	By using a local serial port interface for AP configuration ensures that sensitive management information do not traverse the network as well as minimizing the risk of unauthorized users gaining access via a network protocol used to manage the AP.
47.	Consider other forms of authentication for the wireless network such as RADIUS and Kerberos.	Use of authentication mechanisms such as RADIUS and Kerberos can improve the security and simplify user management.
48.	Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.	Intrusion detection agents (e.g., host-based or networkbased agents) deployed on the wireless network can detect and respond to potential malicious activities.
49.	Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity.	If RADIUS is used, the audit records should be manually or automatically processed to determine if malicious activity has been directed at the authentication server.
50.	Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features.	During product selection, ensure that the product provides enhanced cryptographic protection or user authorization features.
51.	Enable use key-mapping keys rather than default keys so that sessions use distinct WEP keys.	The use of distinct WEP keys provides more security than default keys and reduces the risk of key compromise.
52.	Fully understand the impacts of deploying any security feature or product prior to deployment.	To ensure a successful deployment, an organization should fully understand the technical, security, operational, and personnel requirements before implementation.
53.	Designate an individual to track the progress of 802.11 security products and standards (IETF, IEEE, etc.) and the threats and vulnerabilities with the technology.	An appointed individual designated to track the latest technology enhancements, standards, and risks will help to ensure the continued secure implementation of wireless technology.
54.	Wait for future releases of 802.11 WLAN technologies that incorporate fixes to the security features, or provide enhanced security features.	Upgrade to the latest versions and avoid purchasing the versions of the 802.11 products with major security vulnerabilities that have not been fixed.
55.	When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.	Sensitive or proprietary configuration settings should be cleared from access points before removing them from use or disposing to prevent inadvertent disclosure of the information to potentially malicious users.
56.	If the access point supports logging, turn it on and review the logs on a regular basis.	Ensure that the APs are set to perform logging. Also, review of audit and logging data helps to ensure user accountability.
57.	If the access point supports logging, turn it on and review the logs on a regular basis.	Access point logs should be enabled and regularly reviewed for malicious activity.