Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Wireless Intrusion Detection Systems

This paper will briefly introduce the concept of Wireless technologies, outline the key security threats for wireless networking, specifically focusing on intrusion detection systems for WLAN 802.11 networking and the need for them to be included as part of an overall security solution. Wireless intrusion detection technology, up until recently, has been pushed by the smaller `start-ups' and has been largely ignored by the bigger technology companies. This landscape is changing and I will highlight some of the WIDS sol...

Copyright SANS Institute
Author Retains Full Rights

AD

Wireless Intrusion Detection Systems

GIAC Security Essentials

Certification (GSEC)

Practical Assignment

Version 1.4c

Option 1 - Research on Topics

in Information Security

Submitted by: Ken Hutchison 18 October 2004

Location: GIAC Security Essentials, London, June 21-26 2004

Paper Abstract: The SANS GSEC Whitepaper wish-list made the following statement - Wireless IDS - " small start-ups are pushing the technology and the big players don't even have it on their radars" …

This paper will briefly introduce the concept of Wireless technologies, outline the key security threats for wireless networking, specifically focusing on intrusion detection systems for WLAN 802.11 networking and the need for them to be included as part of an overall security solution. Wireless intrusion detection technology, up until recently, has been pushed by the smaller 'start-ups' and has been largely ignored by the bigger technology companies. This landscape is changing and I will highlight some of the WIDS solutions available, including those from the 'big players' and offer a conclusion on this shift in mindset.

© SANS Institute 2005 Author retains full rights.

Table of Contents

1 Executive Summary 1
2 An Introduction to WLAN Technology 2
2.3.1 PAN – Bluetooth 4
2.3.2 WAN – GSM HSCSD and GPRS 4
3 Wireless Intrusion Detection 8
3.1 What is Intrusion Detection? 8
3.2 Limitations of Intrusion Detection Systems 10
3.3 How to Implement Wireless Intrusion Detection Systems 10
3.4 Open Source Scanning Software 12
3.4.1 Kismet 12
3.4.2 NetStumbler 13
4 Wireless Intrusion Detection Offerings 15
4.1 AirMagnet Distributed 15
4.2 AirDefense 16
4.3 Red-M 18
5 Conclusion 20

© SANS Institute 2005, Author retains full rights

© SANS Institute 2005 Author retains full rights.

List of Figures

Figure 1: WLAN Coverage can often overrun a building's boundaries. 5

Figure 2: Kismet Screenshot showing detected networks
http://www.kismetwireless.net/screenshot.shtml 13

Figure 3: NetStumbler Screen provided by Marius Milner
http://home.pacbell.net/mariusm/ 14

Figure 4: Screen shot source - http://www.isp-
planet.com/img/fixedwireless/2004/airmag-secalarm-policy.gif 16

Figure 5: Screenshot source :
http://infosecuritymag.techtarget.com/images/2002/jul/airdefense.gif 18

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

1 Executive Summary

Hewlett Packard tells us that "*31 Million users worldwide will be accessing public wireless networks by 2007.*"[1]

It is clear that wireless solutions are transforming the way we work and live. Employees are able to keep in touch with their e-mail, calendar and employer from mobile devices, while wireless applications such as Radio Frequency Identification (RFID) Smart Tags are, for example, transforming the way luggage is handled at airports, the way public transport is managed and even tracking cattle to help prevent future bovine disease! Using wireless enabled devices, it is already possible to access the internet from public areas such as coffee shops, hotels and motorway rest stops. All of this is possible through the use of Wireless Local Area Networks (WLAN's).

Businesses of all sizes are also waking up to the productivity benefits and cost advantages of WLAN. Combine this with claims of substantial savings in the reduction of network installation and management costs and the case for deploying WLAN becomes even more compelling.[2]

This has enabled small technology start-ups to afford to develop products and services for WLAN and to allow small to medium businesses to invest in the deployment of WLAN.

So, is it all good news? – Not quite. As with all networks, wired or wireless, the security threats are numerous but with WLAN we need to look at these security threats in a different way – if having network cables run outside the perimeter of your building would make you nervous, then the same concerns should exist where your data is being broadcast over 'air'. The bottom line is that wireless networking, as a new technology, needs new security controls to secure it.

This paper will briefly introduce the concept of Wireless technologies, outline the key security threats for wireless networking, specifically focusing on intrusion detection systems for WLAN 802.11 networking and the need for them to be included as part of an overall security solution. Wireless intrusion detection technology, up until recently, has been pushed by the smaller 'start-ups' and has been largely ignored by the bigger technology companies. This landscape is changing and I will highlight some of the WIDS solutions available, including those from the 'big players' and offer a conclusion on this shift in mindset.

---

[1] HP, page 6.

[2] See WLANA

© SANS Institute 2005 Author retains full rights.

2 An Introduction to WLAN Technology

2.1 WLAN Standard 802.11

A Wireless Local Area Network (WLAN) is a network based on the Institute of Electrical and Electronic Engineers IEEE 802.11 network protocol. As with the Bluetooth standard, it uses high frequency radio waves as opposed to cables and wires to connect network devices. It's called a Local Area Network because the wireless range normally extends to no more than a building or a site and can be measured in hundreds of meters.

A WLAN can be easily built using only a few simple devices:

- A radio transceiver, called an access point (AP) - an AP is essentially a small transmitter and receiver with a wired connection into an ADSL link or Ethernet LAN. It forms an association with a wireless device and acts as an intermediate between the client and the wired connection, providing authentication and seamless access.
- A Network Interface Card (NIC) with 802.11 capabilities which talks to the radio transceiver and allows the data transfer to and from your computer.

The 802.11 protocol also underpins the following common variants of the standard:[3]

- 802.11a – A 5 GHz radio frequency WLAN standard with a data exchange rate of 54Mbps
- 802.11b - The most widely used WLAN standard using a 2.4 GHz radio frequency and a data exchange rate of 11 Mbps
- 802.11g – An improved version of 80211.b using 2.4 GHz radio frequency and a theoretical data exchange rate of up to 56 Mbps.

2.2 Wireless Encryption Standards

Wireless encryption uses security standards which started with the Wired Equivalent Privacy (WEP) standard. This encryption method was introduced in 1999 as part of the 802.11b standard to provide secure wireless communications using the RC4 stream cipher system from RSA. WEP uses a symmetric

[3] See SANS, page 278.

© SANS Institute 2005 Author retains full rights.

encryption scheme where a shared key is used for both encryption and decryption. It was, however, quickly breached and anyone intercepting and monitoring the wireless traffic could easily break the encryption using a brute force attack with tools such as Airsnort and WEPCrack

Programs such as these, crack WEP keys based on an attack described in a paper titled "Weaknesses in the Key Scheduling Algorithm of RC4" written by Scott Fluhrer, Itsik Mantin, and Adi Shamir. This paper identified certain IVs that leak information about the secret key.[4]

Despite WEP's vulnerability, Jon Tullett writing in SC Magazine reports [4] "As flawed as WEP is , a survey of UK businesses by the Department of Trade and Industry found that only one in five wireless networks have WEP enabled".

The SANS Networking Concepts (Security Essentials) page 293 recommends that "WEP is inadequate for protecting wireless networks and that organisations should deploy stronger encryption protocols such as TKIP "

WEP has some use as an obfuscation measure, however, protecting data from casual interception.

The next wireless security standard introduced to try to bolster WEP was Wi-Fi Protected Access or WPA. This standard was introduced last year (2003) and is supported in the more recent 802.11a and g networks. It uses Temporal Key Integrity Protocol (TKIP) as an improved approach to key encryption by mixing the keys.

CISCO System's Lightweight Extensible Authentication Protocol (LEAP) is the last encryption standard we will look at in this paper and it was introduced as an 802.11 standard that allows security authentication data to pass between the AP and a Remote Authentication Dial in Service (RADIUS). This mutual authentication helps mitigate eavesdropping and man-in-the-middle attacks.

2.3 Other Wireless Standards

Although beyond the scope of this paper, I would like to introduce the following types of Wireless technologies, as these can be subject to similar attacks and vulnerabilities as with WLAN.

[4] See Tullett.

© SANS Institute 2005 Author retains full rights.

2.3.1 PAN – Bluetooth

Bluetooth is a short range wireless digital communication technology that provides a Personal Area Network (PAN).

It was developed in 1998 by a special interest group made up of five leading telecom and technology companies as a low cost, low power, way of removing many of the data wires between mobile devices.

Bluetooth communication is used in Mobile Phones, Laptops and PDA's.

Bluetooth uses 2.4 GHz radio frequency, the same as the 802.11b/g network standard (which we will introduce below) and has a data exchange rate of 1Mbps. Its effective range is measured in tens of meters.

2.3.2 WAN – GSM HSCSD and GPRS

The Wide Area Network (WAN) using mobile telecommunications has evolved over recent years from cellular, analogue mobile networks, which used low power wireless transmitters to create wireless cells (where a connected device could travel between similar cells without network interruption) to today's new generation digital technologies which offer a single network standard enabling devices to use voice and data services worldwide.

GSM mobile systems provide higher-speed data transmissions of 14.4Kbps. HSCSD can combine up to four GSM channels and thereby reach a maximum bandwidth of 57.6 Kbps.

GPRS shares free bandwidth capacity of transmitter cells achieving data transmissions of 57.6 Kbps.

With these data transmission rates in mind plus the costs charged by the mobile service providers, WLANs have become a cheaper, faster alternative.

2.4 WLAN Security Vulnerabilities

Having introduced some of the wireless technologies I will now have a closer look at some of the particular security threats to them. Reconnaissance, theft of identity and denial of service (DoS) are not new security threats in themselves, but the confidentiality, integrity and availability in a WLAN does present IT Security teams with new mitigation challenges. This holds true for all IT Security teams, as wireless network access to their network could be installed without their knowledge.

© SANS Institute 2005 Author retains full rights.

By definition, wireless frequencies are designed to be heard by anyone with a wireless receiver – anyone can tune into a wireless network in the same way that they can tune into a radio station. It's this simplicity which makes wireless networks such a potential threat.

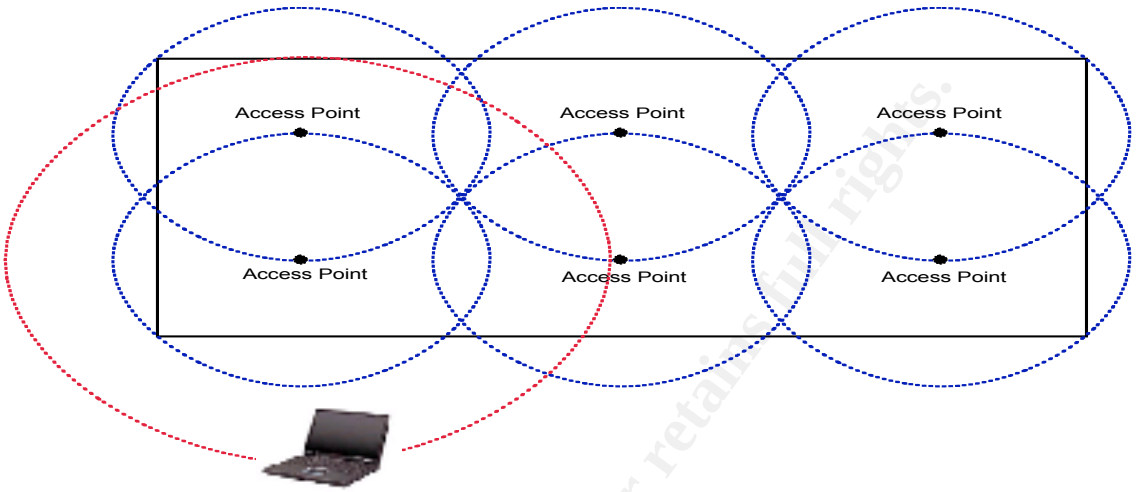

Figure 1: WLAN Coverage can often overrun a building's boundaries.

Let's start with the basic component in a wireless network – the access point (AP) and some of the potential threats to it.

- The signal range of an authorised AP. Figure 1 illustrates how AP signal strength can extend beyond a building perimeter. Consequently, an AP's placement and signal strength have to be calibrated or blocked to make sure the transmitting coverage is just enough to cover the correct area. The RSSI (Received Signal Strength Indicator) on a Laptop wireless card is a good way of measuring wireless coverage inside and outside of a WLAN perimeter. The signal strength needed to make a connection is much higher than that needed to just listen into the network traffic. So by its nature it's a lot easier to just listen than it is to make a legitimate connection.

- The physical security of an authorised AP. Most AP's are mounted on walls or ceilings in clear view, so again, their placement is critical to avoid accidental damage, theft, vandalism or direct access to the physical network cable.

- The rogue, or unauthorised, AP – by placing an unauthorised access point on the network and configuring it to look legitimate, hackers can gain access to wireless user's data. User devices simply connect to the strongest available AP signal and once the association has been made with the rogue AP, the hacker can monitor and manipulate all data that

© SANS Institute 2005 Author retains full rights.

goes through the AP. This is known as 'man-in-the-middle attack'. In built up areas where many WLANS exist, accidental rogue AP association can also cause problems.[5]

- The easy installation and the advantages of having an AP. It is tempting for employees to introduce an unauthorised wireless network onto an internal network to utilise these advantages. This threat also applies to companies who don't even officially use wireless networks.

- The AP configuration. A poorly configured or unauthorised (rogue) AP can provide an open door to the WLAN and can allow a hacker easy entry. By default some AP's can have security controls and encryption switched off.

- Protocol weakness and capacity limits on authorised AP's. These can be subject to denial of service attacks from hackers using rogue AP's when they are flooded with spurious traffic forcing them to reboot or deny legitimate access.

Other security vulnerabilities away from the access point also exist and user indifference to these vulnerabilities, through a false sense of security that distributed wireless connectivity breeds, is one of the other major challenges IT Security faces.

As well as the vulnerabilities at the wireless network layer, weaknesses at the transaction and application layers can also be exploited by hackers.

Finally, the methods used to encrypt wireless data can be breached and the encryption key exposed by hackers intercepting and monitoring wireless traffic. AirSnort is an algorithmic tool which cracks encryption keys on 802.11b Wired Equivalent Privacy (WEP) networks. Airsnort operates on the LINUX platform and

[5] To underline this point I have included an extract from an article by the Boston Business Wire written on September 2nd 2004: "A two-hour war drive throughout New York City on August 24, 2004, using the WiFi Watchdog security solution, provided unique insights into the challenges many organizations face in securing their wireless networks. Highlights of the war drive include:
- A total of 7,039 unique Wi-Fi devices detected, of which 63% were wireless access points and 37% were wireless network cards.
- An average of one wireless network card every 90 seconds accidentally associated with Newbury's unsecured access point (or "honey pot" network) - potentially resulting in a direct connection to the resources on that individual's laptop or PC.
- 67% of the 1,008 unique wireless networks detected near the Republican National Congress site had no encryption enabled, leaving them vulnerable to attacks and security breaches. In fact, Newbury Networks detected 802.11 signals emitted by the Wi-Fi networks of many well-known companies and organizations, including Aetna, Coca Cola, DKNY, Olympus, Applebee's, Starbucks, Burger King, the New York State of Appeals, the New York Film Academy, Columbia University and New York University's Stern School of Business.", Newbury Networks.

© SANS Institute 2005 Author retains full rights.

passively monitors data transmissions, computing the encryption key when enough WEP data packets (hundreds of thousands of data packets) have been gathered.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

3 Wireless Intrusion Detection

It's clear, from the summary of security issues I have highlighted above, that in order to protect our network we need to ensure that we know:

- where **all** access points reside on our network
- what actions to take to close down any unauthorised access points that do not conform to the company security standards
- what wireless users are connected to our network
- what unencrypted data is being accessed and exchanged by those users

To do this we **must** monitor our air space using a Wireless Intrusion Detection System.

3.1 What is Intrusion Detection?

Let's firstly start with the principle and to do this I found the following quote from Ant Allen, research director at Gartner.

"For an enterprise to protect itself from abuse of its information, it must monitor the events occurring in its computer system or network and analyze them for signs of intrusion. To do this, the enterprise must install an Intrusion Detection System (IDS)."[6]

First thing to clarify here is that an IDS is not a firewall! Firewalls are designed to be outward looking and to limit access between networks in order to prevent an intrusion happening. IDS watch the wired and wireless network from the inside and report or alarm depending on how they evaluate the network traffic they see. They continually monitor for access points to the network and are able, in some cases, to do comparisons of the security controls defined on the access point with pre-defined company security standards and either reset or closedown any non conforming AP's they find. The distinction between placing IDS sensors on both wired and wireless networks is an important one as large corporate networks can be worldwide.

[6] Allen.

© SANS Institute 2005 Author retains full rights.

IDS systems can also identify and alert to the presence of unauthorised MAC addresses on the networks. This can be an invaluable aid in tracking down hackers.

In their simplest form, Intrusion detection systems are designed and built to monitor and report on network activities, or packets, between communicating devices. There are a number of tools available which can be used to monitor, capture and decode wireless network traffic. Some are commercial products and some are open source products available on the internet. Some can only capture and store the WLAN traffic, while some can analyse that traffic and create reports with lists of AP's and network devices. Finally, some are advanced enough to analyse signal strength and transmission speed which can be useful in tracking and closing down rogue AP's. In all cases IDS is a vital component in auditing a network installation.

I will look at some IDS products, in more detail, in section 4.

The different types of IDS can be described in the following terms though some products will utilise more than one type:

- **misuse IDS** or **anomaly IDS**: misuse detection or signature based detection as it is sometimes known, looks for network attack sequences or events that match a predefined pattern (or signature). This method is only as good as the signatures provided to it, however, and relies on regular signature updates to keep abreast of known attacks. The advantage of this method is that there are few false alarms, or false positives, when attacks are detected. Anomaly detection on the other hand, relies on the administrator to define normal traffic behaviour on the network – things like typical packet size for example. The sensors then monitor the network for deviations to this normal behaviour and alert when anomalies are discovered. This method can produce a number of false alarms and the systems rely heavily on being 'trained' in what is normal network traffic and what is not.

- **network-based** or **host-based systems**: in a network-based IDS, or NIDS, the traffic flowing through a network is analysed. NIDS is able to detect malicious packets that are designed to be overlooked by a firewall's filtering rules. In a host-based system, or HIDS, the IDS examine the activity on each individual computer. This is done by installing a software client on the host which, again, will detect known attack patterns but only against the host that the client is installed on.

- **passive IDS or reactive IDS:** the passive IDS detects suspicious network traffic, logs the information and signals an alert. A reactive IDS responds to the suspicious traffic by logging off a user or closing down an AP.

© SANS Institute 2005 Author retains full rights.

When we compare 'conventional', or wired IDS, with wireless IDS, the only difference is network topology and the requirement to scan air rather than wire – all the other elements remain the same.

3.2 Limitations of Intrusion Detection Systems

To be effective, IDS must be run online, in real time. Offline, or after-the-event-IDS, is useful for audit trail but will not prevent an attack from taking place. Real time IDS needs to be able to stream data across a network from sensors to a central point where it can be stored and analysed, sometimes known as a correlation server. This 'additional' network traffic running concurrently can significantly impact network performance so sufficient bandwidth is a pre-requisite, though certain tools such as AirDefense Guard allow you to "set rate throttles on each sensor to bring transfer rates to the server as low as 9.6 Kbps."[7]

Today's wireless intrusion detection systems such as AirDefense Guard or AirMagnet Distributed, utilise a misuse, signature, based IDS which has the drawback of only being as good as the signature files and known attack pattern recognition files given to them. This is their basic flaw – you only have protection against what are known to be attacks. The new attack will be the one that gets you, which underlines the need to have an efficient mechanism for keeping all network security components with rule or signature based tables up to date.

All real time IDS system can suffer from issuing false alarms, especially those that use the anomaly based approach. This leads to complacency amongst those members of staff employed to react to or monitor those alarms. The monitoring of IDS alerts is also a 24 x 7 activity and relies on human intervention – as very few hackers work office hours! This is where the big technology players have the advantage over the smaller start-ups – they have the economies of scale which allow them to provide the specialist resources.

To illustrate complacency amongst staff, Bruce Schneier, in Secrets and Lies, tells the story of a 22 hour eBay outage in 1999 "when the IDS system set off alarms constantly, but everyone was too busy to respond."[8]

3.3 How to Implement Wireless Intrusion Detection Systems

Wireless intrusion detection systems will monitor a WLAN using a mixture of hardware and software called intrusion detection sensors. The sensor will sit on

[7] Lindeman/Bulk.

[8] Schneier, page 196.

© SANS Institute 2005 Author retains full rights.

the 802.11 network and will examine all network traffic. The first challenge to be faced when installing IDS is to decide on the best place to locate the sensors. To help make this decision, some detailed analysis must first be carried out on the site of the WLAN:

- What kind of a building or location is it? Steel framed or wooden? (A steel framed building will limit the wireless transmitter's range)
- Are there areas of the site that have to be kept segregated? (In a built up area there will be mixed businesses, or it may be that a payroll department may want to be segregated in a large company for example.)
- What MAC addresses are in use? (This list can be used as a baseline for comparison)
- What authorised Access Points already exist? (Again, this list can be used as a baseline for future comparisons)

Based on this information and from information gathered from sniffing the wireless network - using open source software such as Kismet we can easily build up a picture of what our WLAN looks like – where our AP's are located who uses them, from where and how strong the radio signals are and how strong the radio signals need to be.

We are now in a position to determine where our IDS sensors need to be and to determine how many we need. A 'warwalk' can then be carried out to verify and test the implementation.

Once we have our sensors on the network, the AP's signal strength can be calibrated or blocked to ensure appropriate coverage (see figure1), the network traffic can be analysed and, if we have decided on a misuse type of IDS, can be compared to a signature file for comparison for attack patterns and known vulnerabilities. If an attack pattern is detected the sensor can send off an alert to either a central console, a member of staff or a managed security service provider for appropriate response and action.

In both anomaly and signature based IDS, the systems have to be configured in such a way so as to recognise what is a legitimate network device; say for example a hacker with a rogue laptop enters company premises, and what is not.

In my experience four sensors and one correlation server (the central repository designed to receive the IDS network information) are considered to be a minimum deployment for a small to medium WLAN and this requires the following technical expertise to support it:

© SANS Institute 2005 Author retains full rights.

- IDS Security analysts who can interpret the alerts and make sense of the output
- IDS Software Programmers to program the correlation tools
- IDS Database Administrators

The simplest way to setup a wireless IDS is to use the same open source scanning tools the hackers do. These scanning tools can be divided into active and passive scanning tools where the latter is also known as a 'sniffer'. WLAN scanning software such as Kismet and Netstumbler are freely available on the internet and with a laptop fitted with a Wireless NIC, you have the easiest way of sniffing out **all** AP's on a network to provide a basic IDS.

Analysing and triggering an alarm is done by the IDS software – the action taken in response to the software alert and the architecture and the surrounding processes provide the overall solution and it is here that the bigger technology players (the integrators)have a commercial advantage over the smaller start-ups (the technology innovators).

3.4 Open Source Scanning Software

Open source tools for wireless intrusion detection have become accepted because they are vendor independent.

"Gartner, a leading research and advisory firm, reports that companies will get the most efficient WLAN intrusion detection protection from a vendor-independent dedicated sensor investment. The overwhelming advantage of this method is that all WLAN traffic can be detected regardless of the equipment and vendors involved."[9]

In this section I will introduce the two most common open source wireless scanners.

3.4.1 Kismet

Downloadable from http://www.kismetwireless.net, Kismet is an 802.11a/b/g network sniffer. It is able to monitor networks using almost any card supported in LINUX and Mac OSX operating systems. It works by passively collecting network traffic (listening, not probing) and detecting the standard named networks. Over time, it can also detect hidden networks by analyzing data traffic and building up a 'picture' of data movement.

[9] Studie.

© SANS Institute 2005 Author retains full rights.

Kismet can be used for carrying out site surveys, for detecting wireless networks, access points and signal strength.

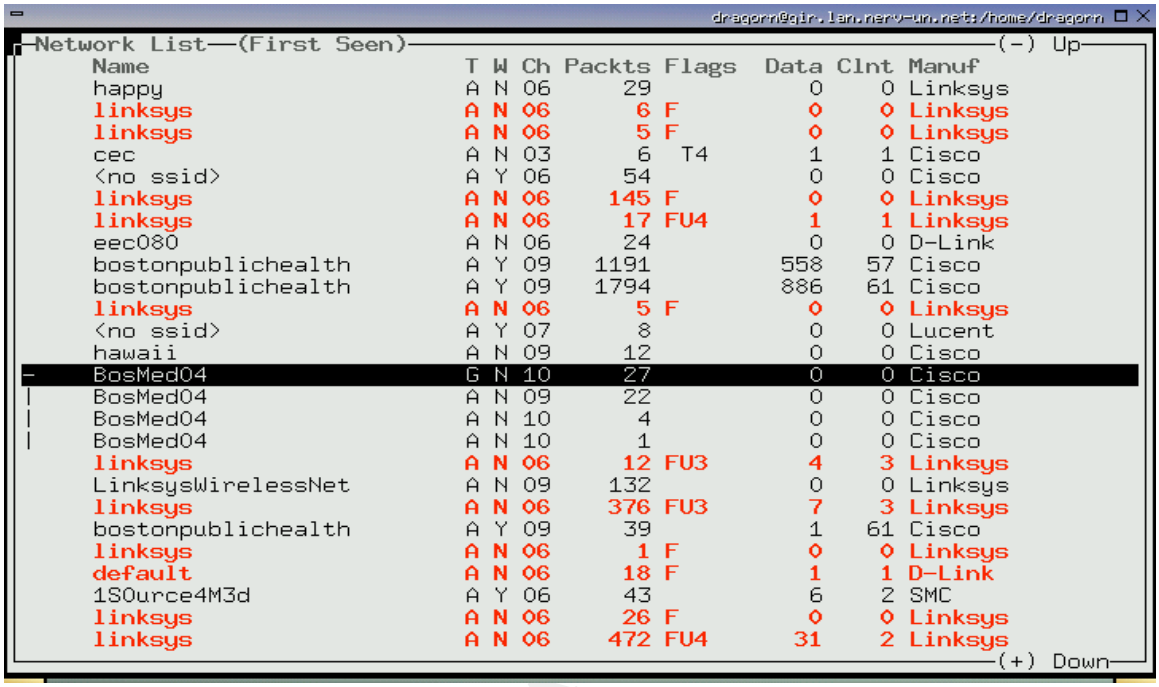

Figure 2: Kismet Screenshot showing detected networks
http://www.kismetwireless.net/screenshot.shtml

3.4.2 NetStumbler

Downloadable from http://www.stumbler.net, Netstumbler is the easiest to setup and most popular scanner used on Microsoft Windows. NetStumbler works by sending 802.11 probes that actively scan by sending out requests every second and reporting on the responses.

AP's by default, respond to these probes, but can be configured not to and to stay silent.

© SANS Institute 2005 Author retains full rights.

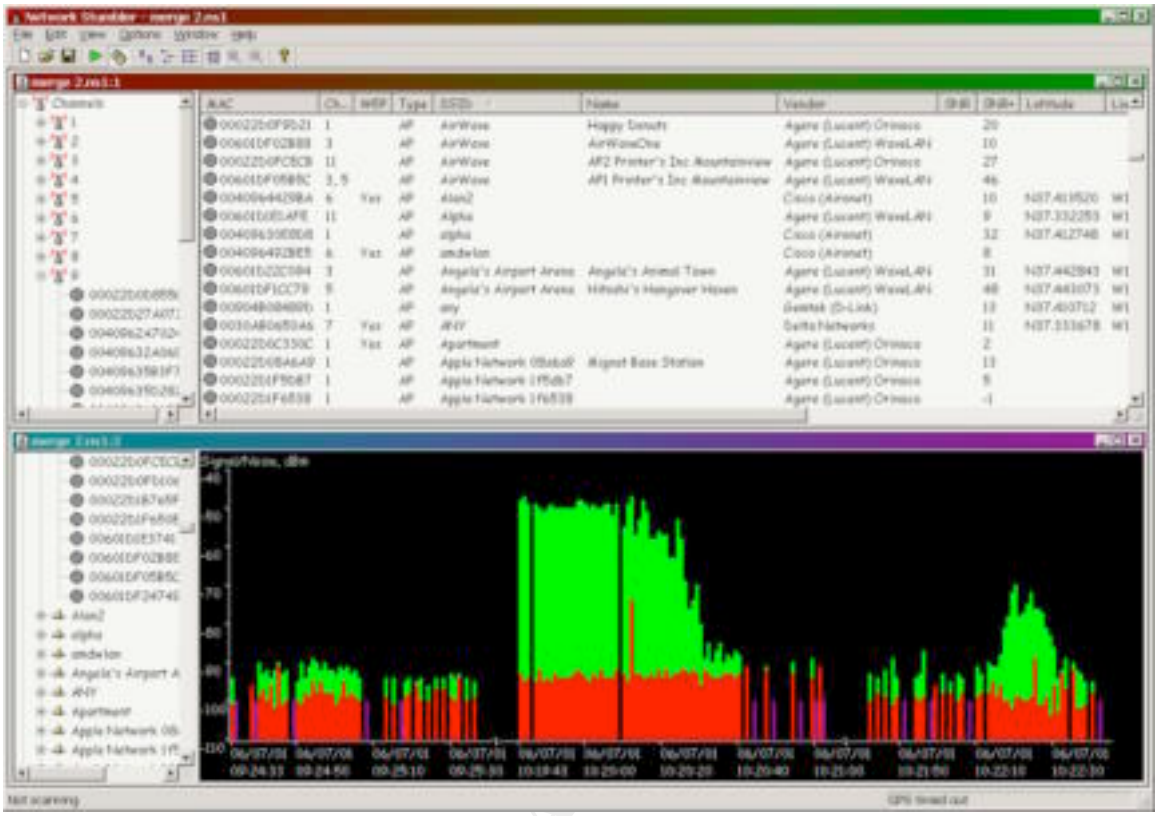

Figure 3: NetStumbler Screen provided by Marius Milner http://home.pacbell.net/mariusm/

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

4 Wireless Intrusion Detection Offerings

The first thing to consider here is – who is going to manage and administer the wireless IDS? If the organisation is big enough, it is likely that the service is going to be run in-house by a network operations group. In this instance 'off the shelf' products such as AirMagnet Distributed 4.0 ,AirDefense Enterprise V4.1 or the Red-M's set of products are well recognised solutions.

If however, the organisation is a small to medium business then it is more likely that a Managed Security Service Provider (MSSP) is the better option.[10]

MSSPs, offer a monitoring and alerting service which will not only gather the network traffic but will offer a 24x7 technical analysis and response to the alert and this is where the bigger technology players have an advantage – by having the technical resources , the hands and eyes, to interpret and respond to any IDS alerting.

IBM's partnering with AirDefense[11], FullMesh and Madge Networks[12] partnering with Red-M, Hewlett Packard with Vernier[13] , Cisco partnering with AirMagnet[14] are all examples of how the big players are starting to move into the market – not through their own product development but through strategic partnerships.

4.1 AirMagnet Distributed

AirMagnet sensors report network performance information and alerts to a management server within a SQL database, which is monitored through a management console. An optional reporting package, AirMagnet Reporter, can generate more than 40 WLAN management reports, from threat summaries to channel RF signal strength.

A review of AirMagnet was carried out by Lyne Borque in March 2004 in Enterprise IT Planet http://www.enterpriseitplanet.com/security/features/article.php/3325971 where she stated "One of the nicer features is the ability to identify and give aliases to various wireless MACs, thus making it easier to identify all actual users and

[10] MSSP's that were providing managed IDS in 2003 are illustrated at http://www.isp-planet.com/technology/mssp/2003/mssp_chart.html.

[11] See AirDefense

[12] See Fairall

[13] See UVPartners

[14] See Cisco1

© SANS Institute 2005 Author retains full rights.

"rogue users". Using the "Find" tool, you can manually and physically track down the location of the rogue user. Much like a Geiger counter, the Find tool will get a stronger signal from the selected MAC as you physically get closer to it. AirMagnet will even pick up DoS attacks as they happen. This can allow for an administrator to disable a site and re-address it. And if the "attacker" is nearby, potentially track them down. "[15]

AirMagnet costs about £2000[16], depending on the version options you decide on.

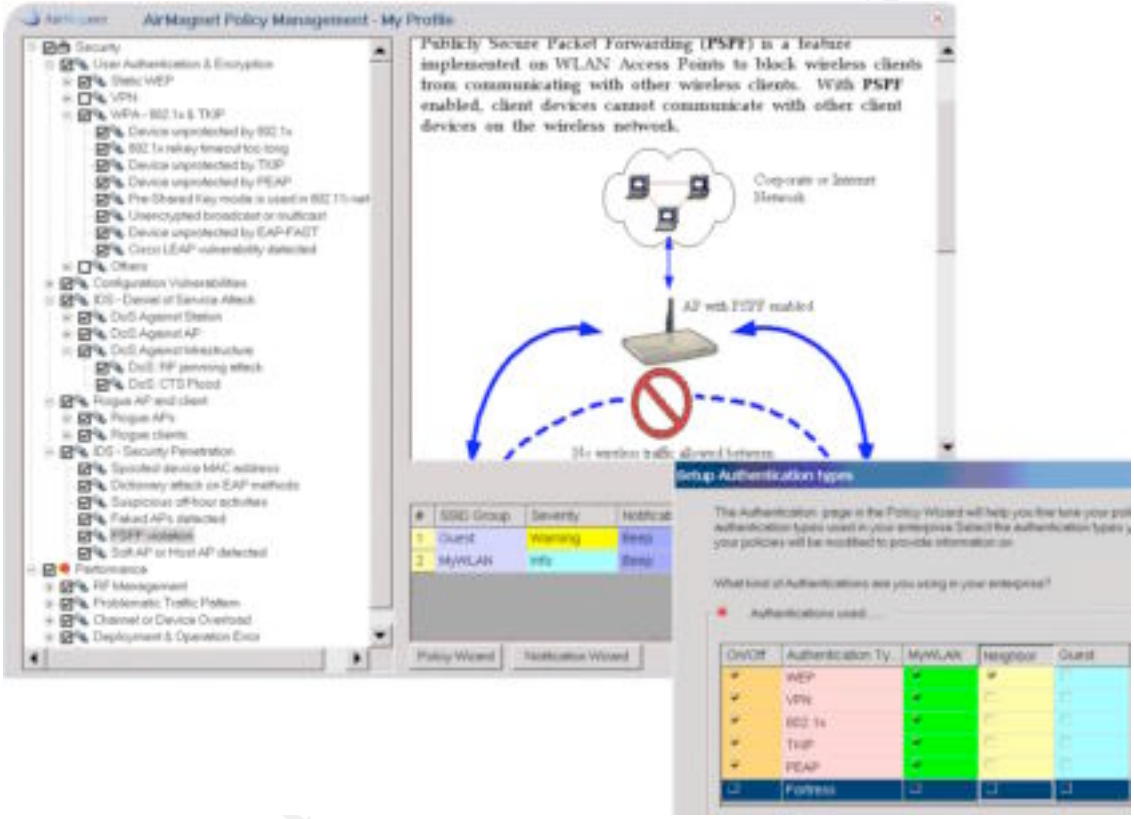

Figure 4: Screen shot source - http://www.isp-planet.com/img/fixedwireless/2004/airmag-secalarm-policy.gif

4.2 AirDefense

The AirDefense system consists of a server running Red Hat Linux with distributed wireless AP sensors and a Java-based Web console. The AirDefense Web console and AP sensors communicate on a secure channel to the server. In

[15] Borque.

[16] Borque.

© SANS Institute 2005 Author retains full rights.

September 2004 IBM partnered with AirDefense to provide their managed WIDS service.

A review of AirDefense 4.0 was carried out by Victor R Garza.[17] Victor states: "Tables and graphs provide views of the entire system with sections for system activity, AP counts, station counts and associations, and ad-hoc activity, as well as graphs of alarms by priority, device, and class. The graphs also include sensor-collected information such as mean signal strength and traffic levels by channel and by bytes transferred. AirDefense's strong suit is its policy-based approach to monitoring wireless devices and traffic. There are four main categories for policies: configuration, performance, vendor, and channel. All of the policy thresholds are configurable. The vendor policy, for example, allows or disallows certain vendors' NICs (network interface cards) and APs from being seen on the wireless network. Knowing which cards are allowed on the WLAN helps prevent session hijacking: If an enterprise only consisted of Cisco NICs, then all other NICs could be excluded so that a non-Cisco NIC would immediately trip an alarm."[18]

AirDefense costs about £5000 for the entry level version.[19]

As illustrated, costs of deploying WIDS solutions such as AirMagnet and AirDefense can be relatively small when stacked up against the risk to a business of unauthorised access.

[17] See Garza.

[18] See Garza.

[19] See Garza.

© SANS Institute 2005 Author retains full rights.

Figure 5: Screenshot source : http://infosecuritymag.techtarget.com/images/2002/jul/airdefense.gif

4.3 Red-M

The Red-M set of wireless security products includes Red-Alert and Red-Vision. Red- Alert is a standalone wireless probe which can detect unauthorised Bluetooth devices as well as 802.11a/b/g networks.

Red-Vision on the other hand is a modular set of products consisting of three main components: Red-Vision Server, Red-Vision Laptop Client and Red-Vision Viewer.

The Red-M website (http://www.red-m.com/Products/Red-Vision/) gives the following explanation of these components:

- **Red-Vision Server**
  This is the heart of Red-Vision and contains both the intra-process communications engine and the internal standards compliant database. It runs on any PC running Microsoft Windows XP Professional and must be TCP/IP accessible from any of the managed devices in the wireless network.

- **Red-Vision Laptop Client**
  This tiny agent is easily installed to run on every laptop computer that

© SANS Institute 2005 Author retains full rights.

connects to your wireless networks. It packs a powerful punch for it's size: it collects data from the end user and also automatically monitors the hardware used, the operating system and configuration changes, software programs installed, data usage, and communication performance. It runs on any PC running Microsoft Windows XP Home or Professional.

- **Red-Vision Viewer**
  The key feature of Red-Vision is an unprecedented innovation in wireless control and security: a geographic based interface. No other wireless software product can offer the wireless network administrator this much control over his constantly changing wireless network from one central console.
  Red-Vision Viewer offers another big plus. No wireless environment features equipment from just one vendor; on the contrary, most feature a great mix of equipment from a variety of vendors. No matter how many different pieces of equipment make up your wireless environment, Red-Vision Viewer gives you this control over every separate device/appliance/hardware type that connects to your network.

Full Mesh Networks are one MSSP that now utilise the Red-M wireless IDS products.[20] Madge Networks are another licensee who re-badge a range of Red-M's wireless intrusion detection solutions along with Red-M's wireless authentication and security technology which is included in Madge's WLAN Enterprise Access Server product.[21]

[20] See Wireless Developer Network.

[21] See Fairall.

© SANS Institute 2005 Author retains full rights.

5 Conclusion

The big technology players now have wireless IDS firmly on their radar's. Managed Security Service Providers (MSSP's) such as IBM, Cisco, Madge and Hewlett Packard all have Wireless IDS Managed Services on offer and the number of off-the-shelf WIDS is rising all the time. Motivating this for MSSP's is the realisation that there is an opportunity to combine the Wireless IDS service into their end to end managed security solution.

I would suggest that this has only come about since wireless network vulnerabilities have been properly understood and wireless networks have been more widely adopted by large businesses. Until recently, the early adopters of the technology have been small to medium business and there simply was not the return on investment for the larger companies to get involved in developing and providing wireless IDS solutions.

What is evident though is that by the time the big players did begin to focus on Wireless IDS there were stronger commercial options available than they could develop themselves. It would seem that they have all considered there to be a better return on investment by partnering with, or buying out, an existing specialist provider.

For example, IBM has this month (September 2004), announced a new managed, wireless IDS service after partnering with AirDefense.[22] They are already in partnership with a startup company Airespace.[23]Okena, developers of the Stormwatch IDS offering were purchased by Cisco and Stormwatch and re-branded as Cisco Security Agent.[24] HP, in turn, have partnered with security start-up Vernier.[25]

To end my paper, I would state that one of the key issues for wireless IDS is that it needs to be supplemented by NIDS / HIDS offerings and it needs to be integrated into an overall network management policy. Consequently, it is here that the smaller start-ups have had to hand the baton over to the big players who have the specialist resources available to provide this.

[22] See Air Defense.

[23] See Jones.

[24] See Cisco.

[25] See UVPartners.

© SANS Institute 2005 Author retains full rights.

References

Air Defense: Air Defense Links with IBM; June 24th 2004; http://www.airdefense.net/newsandpress/06_24_04.shtm 2004-09-30 19:12.

Allen, Ant, Research Director of Gartner: Ward off Data Abuse; http://security2.gartner.com/story.php.id.66.s.1.jsp; 2004-09-17 21:55.

Barken, Lee: WEP Vulnerabilities – Wired Equivalent Privacy? in: How Secure is Your Wireless Network? Safeguarding Your Wi-Fi LAN; August 2003; sample chapter at http://www.phptr.com/articles/article.asp?p=102230&seqNum=10, 2004-09-24 20:13.

Borque, Lyne: Wi-Fi Security Review: AirMagnet; March 2004; http://www.enterpriseitplanet.com/security/features/article.php/3325971; 2004-09-17 21:19.

Cisco1: The Value of the Joint AirMagent Cisco Swan Solution; http://www.terra-wave.com/airmagnet7.pdf ; undated , Cisco Solutions

Cisco: Cisco Systems to Acquire Okena, Inc.; January 24th 2003; http://newsroom.cisco.com/dlls/corp_012403.html 2004-09-30 20:01.

Fairall, Shirley: RedM and Madge Announce Technology Licensing Agreement; September 3rd 2004; http://www.red-m.com/News/news_alert15.asp 2004-09-28 00:12.

Garza, Victor R: May 2004; Wireless IDS's Help Network Admins Keep An Ear to the Air; http://www.infoworld.com/article/04/05/14/20TCwids_1.html; 2004-09-17 22:12.

HP (Editor): HP Wireless Options for Work and Play, 1. Ed. January 2004; http://www.smeforum.org/knowledge/tips/wifi.pdf, 2004-09-14 20:14.

Jones, Dan: Airespace Services IBM; September 16th 2004; http://www.unstrung.com/document.asp?doc_id=59516 2004-09-30 19:19.

Lindeman, Jesse; Bulk, Farnk: Network Computing, March 9th 2004; http://www.mobilizedsoftware.com/showArticle.jhtml?articleId=18311897&pgno=4 ; 2004-09-29 21:37.

Newbury Networks: Newbury Networks Identifies Significant Wi-Fi Security Risks at Republican National Convention Site and Throughout New York City; September 2004,

© SANS Institute 2005 Author retains full rights.

http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20040902005056&newsLang=en, 2004-09-17 20:18.

SANS (Editor): Wireless Networking Concepts - Network Security, Security Essentials V2.2. ISBN 0-9724273-6-8.

Schneier, Bruce: Secrets & Lies – Digital Security in a Networked World; 2000.

Studie , SYSTEMS-world.de, Gartner Says Wireless LANs are the Major Wireless Security Problem Facing Businesses Through 2008, 2004; http://www.systems-world.de/id/6555/CMEntries_ID/51617

Tullet, Jon : 'Take a Leap to a Wireless Future' SC Magazine Published May 2004

UVPartners: Vernier Networks Joins HP OpenView Solution Alliance Program; May 11th 2004; http://www.uvpartners.com/news/v_article9.php 2004-09-30 20:03.

Wireless Developer Network: Full Mesh Networks Launch First Wireless Intrusion Detection and Remote Hacker Shutdown Service; August 10th 2004; http://www.wirelessdevnet.com/news/2004/aug/10/news4.html 2004-09-17 22:12.

WLANA (Editor): The Learning Zone for Wireless Networking, 2004, http://www.wlana.org/learn/roi.htm, 2004-09-14 21:07.

© SANS Institute 2005 Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced