Global Information Assurance Certification Paper

Wireless Security: Considerations, Intrusion Detection Systems, Tools and more

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

Option 1 - Research on Topics
in Information Security

Submitted by: Uday Banerjee
Location: SANS Conference 2004, Virginia Beach

Abstract:

This paper aims to elaborate on security issues faced by the wireless arena, and the emerging technologies that are being used to address them. In particular, this paper is going to take a close look at Wireless Intrusion Detection Systems (WIDS). WIDS is a term that applies to a broad range of technologies and functions that ensure the safety of wireless networks. The security challenges faced by wireless networks include those faced by traditional wired networks, along with others that are specific to wireless systems. This paper is also going to look at some interesting methods and tools that are used to circumvent wireless security in an effort to look at what Wireless IDS systems are defending against.

Introduction to Wireless Security

Wireless networks are fast becoming the norm in organizations of all shapes and sizes. The allure of rapid deployment and simple management is difficult to pass up, when compared to the pains of deploying, administering and maintaining a wired network. There are no faulty cables to look for in a wireless network, are there? But then, network security somehow has a way of making us rethink the utopian dream we just ventured into. Securing a wireless network can be a major hassle. There are well established methods out there to secure a wireless network to the best of one's abilities, but contrary to a wired network, wireless networks are usually all about convenience, and less about most other things. This view is quickly changing to a more realistic one, as more and more people realize that wireless security deserves as much, if not more, attention than its wired counterpart.

Wireless security has many issues to deal with. I have elaborated on a few of them below to build a case for why wireless IDS' should be deployed on every network, wired or wireless.

Weak encryption/No encryption (default settings)

Wireless devices mostly ship with their encryption disabled. It is up to the security-conscious user to dig in and enable the security features on the device. Even if encryption is enabled using WEP (Wired Equivalent Privacy), it has been shown by many people to be insecure [1, 2]. There are a number of tools available to exploit the weaknesses of WEP, such as Airsnort [3] and wepcrack [4].

Misconfigured WAPs

If not configured properly, wireless access points may pose a great threat. There are many settings on an access point which need to be configured in order to enforce good security policies, such as SSID (Service Set Identifier), access control, encryption settings, etc. If these settings are not configured properly, they may serve to jeopardize network security.

Rogue WAPs

Rogue access points can serve to undermine the security of wired-only networks. This is why it is crucial to deploy wireless intrusion detection systems even if a network is meant to be purely wired [5]. A wireless IDS could easily detect a rogue access point by checking to see if the MAC (media access control) address, which is, by design, meant to be unique to every piece of networking hardware, is authorized to be part of a wireless network.

DoS attacks

A DoS (Denial of Service) attack occurs when a service is prevented from being delivered to legitimate users. In the wireless sense, preventing authorized wireless users from being able to access their WAP amounts to a DoS. This may be achieved in one of many ways:

- An attacker floods the WAP with an overwhelming number of association requests, filling up the association table on the access point. If a legitimate user tried to connect to the WAP at this time, he would not be granted access as the WAP's association table would be already full.
- Using signal jamming devices, very much like the ones you find in homes everywhere (microwaves, 2.4 GHz telephones, etc.). Wireless signals tend to get absorbed by obstacles such as walls, thus reducing the effectiveness of the signal. Adding devices that cause interference on the wireless network can only serve to make things worse, and may cause legitimate users to experience a denial of service.
- Using tools such as FakeAP will present the user thousands of access point choices to connect to.

MAC address spoofing

Although it is the intent of network device manufacturers that a MAC (media access control) address is unique to every device, it is a trivial matter to change this address on a given networking card. More detailed information on how MAC addresses can be spoofed, and how spoofed MAC addresses can be detected is elaborated upon in Joshua Wright's paper on detecting Wireless LAN MAC Address Spoofing [6].

Wireless policy not followed

Although many organizations have policies in place to regulate wireless activity, it is a challenging task to enforce this policy. There are many recommendations that can be made with regard to wireless policy [7, 8], such as:

- Disabling SSID broadcast
- Enabling encryption
- MAC filtering
- Static ARP addressing
- Segregating wired and wireless networks, etc.

A wireless IDS can be used as a tool for policy enforcement. It can monitor the airwaves for SSID's, look for unencrypted data from a client/AP, look for unauthorized MACs on the network, and help detect rogue APs, rogue WAPs

and more.

WIDS Architectures

When designing a wireless intrusion detection system, there are some specific considerations that come to mind, such as the ability to cover the entire network, cost of deployment, and non-interference with the existing network. At this time, there are only a handful of WIDS providers, and each of them may have a slightly different approach to the design of their systems. A trial of their offerings may give prospective customers a good idea of what works best for their networks. Alternatively, time and resources permitting, people could design their own wireless intrusion detection system using the many freely available open source wireless tools available on the internet. A good list of open source programs can be found at wi-fiplanet.com [9].

For the purpose of this paper, Wireless IDS architectures may be classified into two broad categories: centralized, and decentralized. A brief description of methodologies and designs being used by some of the key players in the WIDS arena can be found at the unstrung.com website [10].

Centralized Wireless IDS

For a centralized style Wireless IDS, there are several wireless 'sensors' that attempt to cover the entire area spanned by the WLAN (Wireless Local Area Network). The function of these sensors is to gather all wireless data traversing the network, and report it back to a central processing 'analyzer'. This analyzer is the brain of the setup, and carries out the task of scouring the data for patterns of malicious activity, abnormal activity, or activity that conforms to pre-written rules or 'signatures'. Assuming end-users can create their own signatures, or customize existing signatures, it would be possible to accomplish a myriad things, like:

- Check for unauthorized MAC addresses
- Check for rogue WAPs
- Look for high packet error rates
- Look for signal degradation
- Help triangulate an attacker's physical location
- Warn if a WAP's association table is getting filled up above a user-set threshold
- Check for unencrypted wireless transmission

WIDS signatures can take advantage of the fact that traditional wired Intrusion Detection Systems have an established library of signatures that identify a huge number of attacks.

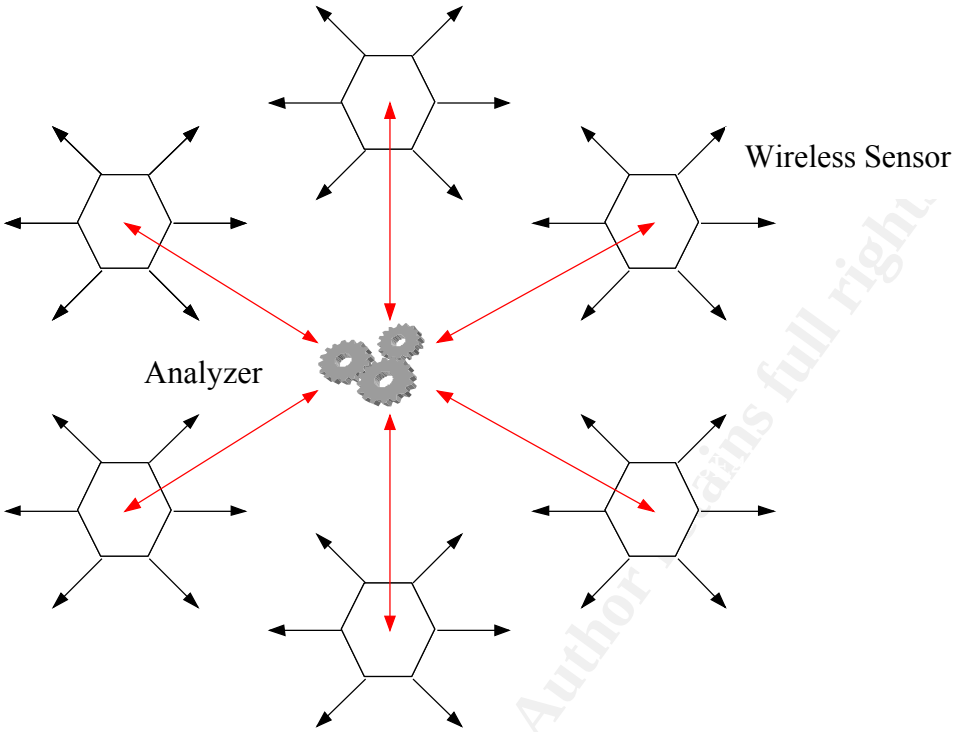

Figure 1. Distributed wireless intrusion detection system scheme

As can be seen from Figure 1 above, the centrally located analyzer will receive feeds from the distributed sensors. The analyzer will process this incoming data and monitor it for signs of malicious activity or activity that does not conform to operating policy. The analyzer will require substantial processing power in order to efficiently process data from large networks. Some of the essential components of a good analyzer would be a competent correlation engine, an excellent rule set, and common sense. Some of the advantages and disadvantages of a centralized wireless intrusion detection system are listed below.

Advantages:

- The centralized model makes it easy to administer protection to large area WLANs. Expansions to the network affect only the analyzer.

- Centralized processing of data allows for a 'big picture' view of what is transpiring on all parts of the wireless network. This allows for quicker damage control, as is illustrated by the following example. If one of the sensors reports that a particular IP/MAC address is attempting to scan its segment of the network, it reports it to the centralized analyzer, which blocks the offending IP/MAC address on all APs (assuming that they have this capability). This reaction may have prevented a compromise on another segment of the network which may have been vulnerable. Although this may only be a short-term solution, as IP and MAC address spoofing [6] are not difficult to perform, it still

gives the network administrator a heads-up on the situation.

Disadvantages:

- At first glance, it is obvious that there is a single point of failure to the above topology. If the analyzer fails, the sensors are rendered useless, and the entire network is now without the protection that the Wireless IDS affords it.

Distributed Wireless IDS

In the distributed scheme, there would be several sensors placed around the network, but there would be no central analyzer. Each sensor would be capable of the functions and capabilities of the analyzer described in the previous scheme. Each sensor would keep in touch with the other sensors to exchange information and alerts in order to function as a coherent setup. The advantages and disadvantages of this type of architecture are listed below:

Advantages:

- No single point-of-failure.

Disadvantages:

- Requirements for each sensor will be hardware intensive

- Overall cost may go up

- Overall coverage may depend on effectiveness of communication between sensors

- Expansions to the network will result in reprogramming all the sensors.

A quick run-through of the advantages and disadvantages of the two systems described above may indicate that the distributed system has more downsides to it than the distributed system, but the distributed system has the most crucial disadvantage of them all, namely a single-point-of-failure. It all comes down to a decision between losing your entire wireless IDS system versus dealing with all the other flaws of a distributed system.

It is also apparent that a Wireless Intrusion Detection System can also be used effectively to enforce wireless policy. Given its ability to spot unauthorized MACs, detect unencrypted traffic, discovering SSIDs, etc., a WLAN administrator could easily track down any offenders of the policy. It would possibly still require him to walk around with a laptop and a wireless card, but the wireless IDS would still provide an early warning. In today's corporate world, where network security is being taken very seriously, a tool such as a wireless

IDS will prove to be the difference between average and good security.

The Other Side of a Wireless Intrusion Detection System

Now that we have looked at the issues present on the inside of networks, and how the wireless IDS system serves to protect it, let us take a look at what lies on the other side. There are all types of people out there who want to get a taste of wireless networks-- casual wardrivers, malicious wardrivers, samaritan wardrivers, etc. These people have access to some powerful tools which can be utilized to sniff your traffic, crack your WEP keys, DoS your network, etc. Some of these tools have already been mentioned in this text, and relate to:

- Sniffing
- MAC address spoofing
- ARP poisoning
- WEP cracking
- Content injection
- Denial of Service, etc.

For the purpose of showing the advanced nature of the tools out there, I have decided to discuss a relatively new tool that was demonstrated at a convention earlier this year. This tool is used for application layer content injection, and is called “Airpwn” [11, 12].

Airpwn

Airpwn is a tool that was demonstrated at DEFCON 12 earlier this year by Bryan Burns and Jacob Appelbaum. We are going to illustrate how this tool can be used to wreak havoc on unsuspecting wireless users. The source code for Airpwn is available at http://sourceforge.net/projects/airpwn. For the curious, the letters “pwn” are to be read as “own” – and “Airpwn” refers to the fact that the victim of this tool was “owned” or was utterly dominated [13].

The syntax for Airpwn, taken directly from the source code, is as follows[11]:

```
airpwn -i <in if> -o <out if> -c <conf file> [options]

  <in if> : interface to listen on (must be in monitor mode)
  <out if> : interface to send packets from (must be in master mode)
  <conf file> : configuration file
  Optional arguments:
        -l <logfile> : log verbose data to a file
        -f <filter> : bpf filter for libpcap
        -h : get help (this stuff)
        -v : increase verbosity (can be used multiple times)
```

A sample command would look like this:

airpwn -i wlan0 -o wlan1 -c /scripts/airpwn/conf/inject -v

where wlan0 is the listening interface and wlan1 is the interface that will perform the injection. We would require two wireless cards to be able to perform any of the actions described below. As specified, the listening interface must be in 'monitor mode', which means that the interface can sniff packets without associating itself with a wireless access point [14]. This is useful from attackers' perspective because they need not identify themselves, nor make any transmissions that may help pinpoint their location. The injecting interface is required to be in master mode.

Airpwn monitors the airwaves for traffic, and when it intercepts requests that match a specified request, it returns a pre-configured response. These settings can be modified in the configuration files in the /airpwn-0.50c/conf/ directory. Because Airpwn has been listening in monitor mode, it knows what sequence numbers, source IPs, and MAC addresses to use when injecting a response. As explained by the authors of this program in their 'readme' file, Airpwn will work only if it responds with a smaller latency when compared to the real data source. Airpwn depends on the following packages in order to work properly: libpcap (packet capture interface), libnet (generic networking API), libpcre (perl compatible regular expression library), and hostap drivers (Linux drivers for certain wireless cards).

This tool can be used to bring the world of 'phishing' [15] emails to a more dangerous realm. Imagine a situation where we have a malicious person sitting around waiting for people to access their bank's website. The users would get a webpage that looks exactly like their bank's website, only this time it is a cleverly disguised webpage whose only intent is to collect usernames and passwords. An obvious answer to this problem would be to enforce the use of encryption on the wireless network. This would make it a lot more difficult for the person sitting outside your wireless network to be able to inject content into your network if he cannot make sense of the data that he/she sees. But if this tool is used in conjunction with existing tools like Airsnort [3] and wepcrack [4], the attacker can use these password cracking tools to crack the encryption key, and then use it to perform injection into the victim's network. From the perspective of wireless IDS systems, this type of attack could possibly be detected using signatures that look for unnaturally quick responses from web-servers combined with reset packets being sent back to the same web-server.

On another note, it is fast being realized that WEP is insecure, and many networks are making the transition to WPA (Wi-Fi Protected Access) and the more secure WPA2 security scheme [16]. WPA2 uses AES (Advanced Encryption Standard) [17] to perform data encryption, which is a much more robust and stronger encryption method when compared to the other solutions in the field. The use of fresh session keys also makes WPA2 more secure than

the rest of the protocols currently being used to secure wireless networks.

Future Directions

The field of wireless IDS is quite nascent, and there is great scope for development and improvement. As with the field of wired intrusion detection systems, wireless systems will need to make the leap toward Intrusion *Prevention* Systems (IPS). Intrusion prevention essentially marries the capabilities of an intrusion detection system with the capabilities of a firewall. There are several approaches to the design intrusion prevention systems. Some of them are listed below [18]:

- Inline devices: These are devices that sit 'in-line' with the traffic entering and leaving the network. They are usually layer 2 devices which inspect inbound and outbound IP packets for patterns associated with malicious activity. If the data in a packet matches a pre-written rule or signature, the IPS will drop the malicious packet and alert the concerned parties of the attack.
- Application firewalls: This class of IPS would comprise software that acts like a personal firewall to an application. An excellent example would be ModSecurity [19], which is an intrusion prevention system designed for web applications. It is designed to run as an Apache module and pre-processes all inbound data, looking for content matches. Users can configure any number of content strings in the Apache configuration file for ModSecurity to look at. Users who are currently not using anything other than a firewall may benefit greatly from using a product like ModSecurity.
- Host based Intrusion Prevention: This flavor of Intrusion Prevention covers just the host machine they reside on. One popular example of a host based IPS is the Cisco Security Agent [20]. A distinct advantage of this product is that it analyzes behavior to arrive at decisions on whether to block something or not. The disadvantage of this approach is that only one host is protected.

Integrating intrusion prevention technology with wireless networks may be a bit of a challenge. This would mean integrating existing wireless equipment with intrusion prevention systems. Given that today's hardware based Intrusion Prevention Systems require a considerable amount of processing power, it is quite unreasonable to expect current wireless routers and access points to perform the same tasks. However, IDS/IPS engines are improving by the day, while hardware performance and power are seeing a tremendous increase as well. It should not be too far into the future when fully integrated wireless intrusion prevention systems are offered for consumer use.

Conclusions

It is evident that networks of all types and sizes will benefit greatly from the use of wireless intrusion detection systems. Wireless intrusion detection systems have the capability to be used as an effective policy monitoring tool. Open source wireless IDS programs provide great alternatives to some of the extremely expensive commercial tools available, and so wireless IDS adoption is not going to be cost prohibitive. There are more and more advanced tools being released that can seriously undermine wireless security, and unless a network has some sort of a detection mechanism, it will be quite a challenge to keep oneself informed of what is transpiring on one's network. Finally, users on wireless networks must be educated with respect to the wireless acceptable use policy, risks pertaining to wireless use, and good practices to implement while using a wireless network connection. There is no substitute for good education – and I believe ensuring that wireless users are well educated will help maintain a secure wireless network. But since we cannot take a chance on that, I believe Wireless Intrusion Detection Systems are here to stay.

List of Figures

References

[1] Fluhrer, Scott, Mantin, Itsik, and Shamir, Adi. "Weaknesses in the Key Scheduling Algorithm of RC4", in Proceedings of SAC 2001. (2001)

[2] Roos, Andrew. "A Class of Weak Keys in the RC4 Stream Cipher", in sci.crypt.research. (1995)

[3] Airsnort homepage. URL: http://airsnort.shmoo.com/ (2003)

[4] Wepcrack Sourceforge page. URL: http://sourceforge.net/projects/wepcrack (2003)

[5] Shimonski, Robert J. “Wireless Attacks Primer”. URL: http://www.windowsecurity.com/articles/Wireless_Attacks_Primer.html (Feb. 24, 2003)

[6] Wright, Joshua, Detecting Wireless LAN MAC Address Spoofing, page 15, URL: http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf (Jul. 26 2003)

[7] Farshchi, Jamil. Wireless Network Policy Development (Part One) URL**:** http://www.securityfocus.com/infocus/1732 (Sep. 18 2003)

[8] Farshchi, Jamil. Wireless Network Policy Development (Part Two). URL**:** http://www.securityfocus.com/infocus/1735 (Oct. 2 2003)

[9] Phifer, Lisa. Open Source WLAN Analyzers. URL: http://www.wi-fiplanet.com/tutorials/article.php/3383441 (Jul. 20 2004)

[10] Brown, Gabriel Wireless IDS Is All the Rage. URL: http://www.unstrung.com/document.asp?doc_id=42313 (Oct. 22 2003)

[11] Burns, Bryan and Appelbaum, Jacob. URL: http://sourceforge.net/projects/airpwn (2004)

[12] airpwn - bringing goatse (and friends) to Defcon 12! URL: http://www.evilscheme.org/defcon/ (2004)

[13] Urban Dictionary, definition 1. URL: http://www.urbandictionary.com/define.php?term=pwned (2003)

[14] Airsnort FAQ's. URL: http://airsnort.shmoo.com/faq.html#Q3 (2003)
[15] What is phishing? URL: http://www.webopedia.com/TERM/p/phishing.html (Sep. 15 2004)

[16] WPA2. URL: http://www.wi-fi.org/OpenSection/protected_access.asp (2004)

[17] Announcing the Advanced Encryption Standard. URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (Nov. 26 2001)

[18] Desai, Neil. Intrusion Prevention Systems: the Next Step in the Evolution of IDS. URL: http://www.securityfocus.com/infocus/1670 (Feb. 27 2003)

[19] Ristic, Ivan. ModSecurity website. URL: http://www.modsecurity.org

[20] Cisco Security Agent website. URL: http://www.cisco.com/en/US/products/sw/secursw/ps5057/