Global Information Assurance Certification Paper

Wireless Honeypot

Rick Schoeneck

GIAC Security Essentials Certification (GSEC)

Version 1.4b
Option 1

June 8, 2003

Table of Contents

Abstract

Wireless local area network (WLAN) technologies have really taken off in the last few years. Large corporations to beginning home users are implementing WLAN's because of their low cost, ease of implementation and flexibility of deployment. But, as recent media articles have been hyping, WLAN's are inherently less secure than their wired counterparts, mainly due to the physical security aspects of the technology, but also because of weak encryption and authentication implementations. New and more sophisticated wireless LAN hacking tools are being released frequently. We security professionals need to try and stay ahead of the game by implementing strong security measures, ensuring that intrusion detection systems are being deployed, and deploying wireless honeypots. Wireless honeypots are a way to try and stay ahead of the hacker community, helping to determine the latest tools and techniques being used by the hacker community.

This paper will journal some of the latest activities in the honeypot community related to WLAN's and discuss the components of a wireless honeypot.

Introduction to Wireless Local Area Networks

There are a number of wireless local area network technologies available today (802.11, Bluetooth, and HomeRF) with 802.11 emerging as the predominate technology. The focus of this paper will be 802.11 technologies. 802.11 refers to the Institute of Electrical and Electronics Engineering (IEEE) standards related to wireless local area networks (WLAN). Anytime you start talking about 802.11, you will end up trying to decipher an alphabet soup of standards and acronyms, so let's run through some of them quickly.

The primary standards that relate to equipment connectivity are 802.11a, 802.11b, 802.11g and 802.11b+.

802.11b also known as WiFi (Wireless Fidelity) is the predominate implementation to date. It operates in the 2.4 Ghz frequency range and can achieve theoretical bandwidths of up to 11 Mbps. Bandwidth is dependent on distance between the wireless devices, physical barriers (doors, walls, etc.) and interference from other devices. The 2.4 GHz frequency range is unlicensed frequency spectrum that is used by numerous other devices like microwave ovens, cordless phones and baby monitors. So interference issues can exist and the Federal Communications Commission has mandated very low power restrictions. As such, the range of 802.11b is around 200 – 300 feet.

802.11a operates in the 5 GHz frequency range which is less frequently used and therefore suffers less from interference issues. 802.11a technology can achieve theoretical bandwidths of up to 54 Mbps, again, dependent on distance between the devices, physical barriers and interference from other devices. With the higher bandwidth capacity, one would expect that this would be the preferred

technology. But, a number of factors including a lower range, higher initial cost compared to that of 802.11b and the fact the bottleneck in a typical consumer's network would be their internet access (typically less than 2 Mbps) has led to 802.11b dominance. There are instances where 802.11a implementations may be better suited. For additional information on the comparisons of 802.11a and 802.11b see the article "Wireless Comparison Information" [7] or for a more technical comparison see "802.11b/a - A physical medium comparison" [4]. Because of the higher frequencies, a range of up to 75 feet is more common for 802.11a, which is significantly less than that of 802.11b.

802.11g is still a draft IEEE standard. But, according to IEEE news releases, "IEEE P802.11g … Final Approval Expected in June 2003" [5] the standard should be finalized soon. Hardware vendors are not waiting for the final approval though. The 802.11g standard is backwards compatible and new equipment is already on the market that supports both 802.11g and 802.11b technologies. 802.11g uses the same frequency spectrum as the popular 802.11b (2.4 GHz), but can achieve bandwidths of up to 54 Mbps by using orthogonal frequency division multiplexing.

802.11b+ is a new development in equipment technology. There is no corresponding IEEE standard, rather, Texas Instruments used packet binary convolutionary coding as a way to extend theoretical bandwidth of 802.11b technologies to a capacity to 22 Mbps. 802.11b+ devices are compatible with 802.11b devices, but you will only achieve the increased bandwidth if both communicating devices are using 802.11b+ technologies.

Below is a summary of the major communicating 802.11 technologies:

	802.11b	**802.11a**	**802.11g**	**802.11b+**
Frequency	2.4 Ghz	5 Ghz	2.4 Ghz	2.4 Ghz
Theoretical Bandwidth	11 Mbps	54 Mbps	54 Mbps	22 Mbps
Actual Bandwidth	3 -5 Mbps	20 - 27 Mbps	20 -25 Mbps (TBD)	6 – 8 Mbps
Range (max.)	300 ft.	75 ft.	300 ft.	300 ft.
Interference	Heavy (cordless phones, microwaves, baby monitors)	Moderate	Heavy (cordless phones, microwaves, baby monitors)	Heavy (cordless phones, microwaves, baby monitors)
Market Penetration	Strong user base, most public access uses this standard, many new laptops incorporating this technology	Products are available but not much of a take up by consumers, some business use	New products just starting to hit the market	New products just starting to hit the market
Standards Approval	IEEE approved 1999	IEEE approved 1999	IEEE approval expected in June 2003	None
Equipment Costs	AP* $100 Adapter $50	AP* $150 Adapter $50	AP* $130 Adapter $70	AP* $90 Adapter $60

*Access Point (AP)

Next, I want to review some of the acronyms related to security again, more alphabet soup.

Wired Equivalency Privacy (WEP) is the optional encryption mechanism that is available in most of today's wireless products. While any encryption is better than no encryption, WEP has proven to be a weak implementation and there are readily available free tools that allow a hacker to break into a WEP protected network in a very short timeframe.

802.1X is a new framework for authentication and key management. Jim Greer gives the following description of 802.1X:

> The use of IEEE 802.1X offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1X ties a protocol called EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication. [2]

WiFi Protected Access (WPA) is a near-term, security implementation based on a subset of IEEE's 802.11i standard (see below). It is being driven by the WiFi Alliance and new products are currently undergoing certification. It is designed to run on equipment that currently supports WEP through software/firmware upgrades. It will improve security through enhanced data encryption using Temporal Key Integrity Protocol (TKIP) and improve user authentication via 802.1X and the Extensible Authentication Protocol (EAP).

802.11i has three primary components to the standard as stated by Dennis Eaton in is article "802.11 Security". [13] The first component is improved encryption algorithms in the form of Temporal Key Integrity Protocol (TKIP) and the Counter Mode with CBC-MAC Protocol (CCMP). The second and third components address primary weaknesses of WEP, authentication and Key distribution by implementing the 802.1X framework. The 802.11i standard also sometimes referred to as Robust Security Network (RSN), is still in draft and expected to be finalized late in 2003.

There are two primary modes of operation for WLAN's, Infrastructure and Ad-hoc. Architectures that use an access point are referred to as using infrastructure mode; peer to peer wireless networks are referred to as using ad-hoc mode.

The primary security difference between wired LAN's and wireless LAN's is that with wired LAN's you need to either gain access to the physical wiring or achieve some method of network connectivity to compromise the network. Access to the physical network is usually protected by buildings, with guards, door locks, access badges and other physical security measures. External network connectivity is typically protected by firewalls and well configured routers. With wireless LAN's, on the other hand, proximity to other devices is all that is needed. Depending on the deployment, a hacker might be on a nearby floor, just outside the building, or sitting in a car parked hundreds of feet away from the devices, and still be able to gain access to the network traffic. And, don't think that just because you have not deployed a wireless network that you don't have to worry about wireless security. Many laptop vendors are incorporating WiFi into their standard systems and the unsuspecting user who has used his/her laptop at the local coffee shop's WLAN may have left their laptop configured in a manner that makes them susceptible to intrusions. For these reasons, and the current weak state of WLAN encryption and authentication, you need to be concerned.

The purpose of this paper is not to review every aspect of Wireless LAN's or every aspect of the 802.11 standards. For more information related to 802.11 standards, see the article titled "802.11 Alphabet Soup". [3] It is also not my intention to detail all of the security short comings of the current 802.11 implementations. There are many good articles on that in the SANS reading room, or one of my favorite wireless security sites (http://www.loud-fat-bloke.co.uk) has an excellent article "802.11 Security – The Attacks Explained". [8] One additional reference, "Advanced 802.11b Attack" is an often referred to presentation by Robert Baird and Mike Lynn [14] that was delivered during the 2002 Black Hat Briefings in 2002. It is a good presentation but lacks the speaker notes which would make it an excellent resource. This overview of terminology, will aid you in further researching 802.11 technologies and security issues. Suffice it to say that wireless security is lacking today and we need to monitor the activities occurring on our WLAN's.

Honeypots

A honeypot is a system designed to be broken into in order to lure an intruder away from other more valuable systems and to log and monitor the activities of the intruder. Honeypots emulate systems or services that a hacker would typically target (ftp services, web servers, firewalls, routers, etc.). Lance Spitzer categorizes honeypots into two types: low-interaction and high-interaction. [12]

A low-interaction honeypot would be characterized by its minimal interaction with the hacker. These types of honeypots typically emulate a specific service like ftp or http. They are much simpler to deploy and maintain, but log only a limited amount of information regarding the hacker's activities. One additional advantage is that since these systems are only emulating certain services they reduce the risk of an attacker using these systems to compromise other down-stream systems. Examples of low-interaction honeypots include: Specter (http://www.specter.com), Honeyd (http://www.citi.umich.edu/u/provos/honeyd), and KFSensor (http://www.keyfocus.net/kfsensor).

High-interaction honeypots are much more complex than low-interaction honeypots and typically include giving the hacker access to the Operating System. This gives the hacker a real system to interact with and thus you can capture much more information about the hacker's activities. With a low-interaction honeypot you try to restrict the activities of the hacker to the services that you have emulated and are logging, but with high-interaction honeypots you let the hacker run free logging their every activity. One major disadvantage of this is that the hacker could compromise the honeypot and use it to attack other systems; leaving you liable for allowing the hacker access. Additionally high-interaction honeypots are very complex to deploy and maintain. Examples of high-interaction honeypots include Symantec Decoy Server (http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=157&EID=0) and Honeynets (http://www.honeynet.org).

There has been a recent debate on the legality of implementing honeypots. Are they a form of entrapment or measure of defense to protect your computing equipment and data? This author is not providing legal advice, but in my opinion, with the proper deployment and warning banners, it would seem that a honeypot would serve as a legal tool to assist in protecting your information technology assets. For a more detailed discussion about the legality of honeypots, see the article “Use a Honeypot, Go to Prison?” [10]

Wireless Honeypot News

As I mentioned earlier in this paper, articles on the insecurity of wireless LAN’s abound. But, two recent articles have journaled the implementation of wireless honeypots and both are touted as ground-breaking steps to chronicling the vulnerabilities of WLAN’s. The first article is about a project conducted by SAIC in Washington DC dubbed WISE (Wireless Information Security Experiment). This implementation used high-end Cisco equipment, high-gain antennas, vulnerable bait systems, logging hosts, a 802.11 sniffer system and a customized intrusion detection system. Unfortunately, SAIC reported that very little interesting activity has been recorded to date. For more details on the WISE project, you can read the article “Wi-Fi Honeypots a New Hacker Trap”. [11]

In the second article, a little more traffic was recorded by the consulting firm KPMG in London, England. Some interesting characteristics were inferred about the wardriving hackers.

> Most do it as a hobby, and in some case to use the network to access the Internet… The most popular time for war driving was between 9-10 am, where 24% of probes took place, and 5-6pm where 18% of probes took place. This suggests that people scan for wireless access points while driving in cars, or while on foot or cycling. Virtually no activity was recorded at weekends [6].

While this may seem harmless, wireless vulnerabilities are significant. Hacker tools are prolific, and the ease at which one can gain access to the traffic should make one ensure that risks are clearly analyzed before implementing a WLAN in any critical business activity. The risk assessment must not overlook the risk of impacting business partner or consumer confidence. In the case of the recent Best Buy incident, they had implemented mobile Point of Sale (POS) Terminals that used 802.11b, but apparently “did not use even the most fundamental security features of WiFi”. [1] A researcher was able to sniff the wireless network and capture sales transactions, including what appeared to be credit card information. Best Buy was not completely dependent on their Wireless POS terminals, so business activities did not have to be shutdown, but the incident tarnished their image and may have impacted sales in the immediate time frame.

We must be diligent, we must monitor our wireless networks and we must get smarter about the exploits.

Wireless Honeypot using wired tools

You could create a wireless honeypot system based on the current tools available today. When I started this project, I thought this would be the only practical way to initially experiment with capturing the activities of wireless hackers. If you have experience with some of these tools or just want to wait around for the next generation of open source or commercial wireless tools, this is still a viable option, although you will be missing some very critical information. You could use a standard Access Point (AP) with logging capabilities, a network sniffer/logger (e.g. snort - http://www.snort.org) and any of the current wired Honeypots listed above. This would give you the basic capabilities to monitor wireless hacker activities, and if you made this a completely stand-alone environment, all of the activity would be considered suspicious activity to be analyzed. Most AP's log, at a minimum, all attempted associations along with the MAC address of the wireless clients. This would provide you with the traffic patterns and frequency with which attempted access was made.

It would be interesting to configure the AP at first with no encryption or security measures in place, and then, incrementally add WEP, MAC address filtering and other security measures to identify the sophistication of the wireless hackers. For this to be successful, it would probably require that you be in an area with frequent exposure (e.g. near a popular open public WLAN) or that you provide some valuable resource that would keep an attacker coming back (e.g. true internet access).

As discussed in some of the already referenced articles on Honeypots, the risk of providing real resources is that they could be used to conduct attacks on other systems and you could be held liable. Again, this is not a legal advice project. Do your due diligence to protect yourself before taking such actions.

Based on the activity detected on your wired honeypot and network sniffer you could infer the intent of the hacker:

- No activity on the wired honeypot (but association with the AP) – a casual wardriver merely cataloging the location (but this could also be for planned future activities).
- Attempts to gain internet access only – a casual wardriver or freeloader looking to gain free internet access (but again this could also be for planned future activities).
- Installation of backdoor or other hacker tools – this might be a more sophisticated hacker looking to compromise a system for future hacking activities.
- Overwriting or deleting key system files – malicious intent to compromise and inflict damage to information systems.

Because a wired network sniffer would only detect an intrusion after the hacker had been associated with the AP, the detection of many suspicious activities (AP scanning, Denial of Service attacks against the AP, spoofed AP's, etc.) would likely be missed thus a wireless intrusion detection and honeypot capability needs to be developed.

Wireless Honeypot design and tools

With the wireless honeypot using wired tools, you could create all of the necessary honeypot aspects of a wireless honeypot (the honey to draw a would be attacker in). A typical hacker is not looking to gain access to the AP, but rather the resources beyond the AP. As of this date, I have not read of any viruses, Trojans, or other malicious code that would reside and operate on an AP. Although, as time passes, I would expect to see the development of new attacks that would log all of the associations and traffic passing through a compromised AP or to use the AP to spread malicious code.

You could create an additional avenue for exposure by setting a wireless client device in ad-hoc mode and placing wired IDS or honeypot software on the machine. But, again, the resource to be exploited would be the client PC and probably not the wireless adapter. So the current wired tools would work just fine.

What is needed, in a wireless honeypot, is the ability to log activity at the media access layer related to the discovery and association to the AP. I am not a programmer by trade and never had any delusions that I would be able to create such a tool. When I started this research project I expected that I would have to identify already existing tools or describe the needed features of such a tool. But, I could not find tools that were self described as a wireless honeypot. Very late in my research, I discovered an informative website by Mark Osborne (http://www.loud-fat-bloke.co.uk).

Mark appears to have the programming background and security experience to tackle such a project. I have found Mark's articles very easy to understand and sprinkled with enough British humor to keep them entertaining. His diagram "1.2 Attack Direction – the object of desire" on page two of the already referenced document "802.11 Security – The Attacks Explained" [8] shows 4 targets of a wireless attack. Target one is the typically thought of target, the corporate network beyond the AP. The second target is the exposed official client machines already associated or attempting to associate to the Official Access point. The third target would be the official access point, and the fourth, any rogue access points. Mark goes on to explain a number of 802.11 vulnerabilities in this paper. If you haven't read it yet please do.

Mark has created a Wireless Intrusion Detection System (IDS) that fills the need of logging the activity at the media level related to the discovery of and

association to the access point. Mark's tool, WIDZ (Wireless Intrusion detection system), has the beginnings of an Open Source tool to fill the current gap in wireless security detection. By his own claims, his software is still in the proof of concept stage and is being made available to be run under lab conditions. The source code, design documentation and a readme file can be downloaded in a zipped format from his website http://www.loud-fat-bloke.co.uk/tools/widzv1.5.zip . The current version 1.5 detects:

- Rogue AP's
- Monkey/Hacker Jacks
- Null Probes
- Null Associations
- Bad MAC ID's (via MAC black list)
- Bad SID's (via ESSID black list)
- Floods

There are already planned enhancements for a version 2 that include:

- AP Scanning Techniques
- Signal Strength Changes
- Detection of MACs with the strings EA7 or BAD
- OS fingerprinting
- And more

There are other commercial Wireless IDS's like Airdefense (http://www.airdefense.net), but for those of us with limited budgets, Open Source tools are sometimes a necessary option.

Like I mentioned earlier, when I started this research project I thought I might need to describe the requirements of a wireless honeypot, and I had some grandiose ideas that if you could create one system (a laptop with a wireless card) that would act as the AP, the client, the IDS and the honeypot, it would be ideal for the ease of deployment. And, if the system could simulate not just one, but many wireless clients so as to project a very busy WLAN, that would certainly help to gain the attention of wireless hackers. But since there are people like Mark on the job, I will leave the requirements definition to the people that might have a clue as to whether or not it is technically feasible.

Conclusion

It seems that most would concur that the state of wireless security is inadequate, yet, WLAN's continue to be deployed. And, for the home user surfing the web and sending emails or to address certain mobility issues in the corporate world, the current state of security may be adequate if properly deployed. Standards bodies and manufacturers continue to further the security advancement of WLAN's with features like WPA and 802.11i. But, we need the tools to do our jobs as Information Security professionals, and a Wireless IDS to support a Wireless honeypot is needed. I believe Mark Osborne is on the right track with

his Open Source tool WIDZ. He may flame this paper for being “Incredibly high-level” and “[of] which is of no practical use to most of the business world who all use a computer on a daily basis.” [9] But, a person needs to start somewhere and my hope is to add to the awareness of the security community and to get those with the necessary skills to add to Mark’s work in developing an Open Source wireless intrusion detection system.

References

[1] Gallagher, Sean. “Best Buy: May Day Mayday for Security”. 7 Jun 2002.
URL: http://www.baselinemag.com/article2/0,3959,95806,00.asp
(8 Jun 2003)

[2] Geier, Jim “802.1X Offers Authentication and Key Management”. 7 May 2002.
URL: http://www.80211-planet.com/tutorials/article.php/1041171
(7 Jun 2003)

[3] Geier, Jim. “802.11 Alphabet Soup”. 5 Aug 2002.
URL: http://www.80211-planet.com/tutorials/article.php/1439551
(7 Jun 2003)

[4] Hansen, John. “802.11b/a - A physical medium comparison”. 1 Feb 2002.
URL: http://rfdesign.com/ar/radio_ba_physical_medium/
(7Jun 2003)

[5] IEEE. “IEEE P802.11g (TM), 54Mbps Extension to 802.11b Wireless Local Area Networks, Gains Working Group Approval Final Approval Expected in June 2003”. 14 Feb 2003.
URL: http://standards.ieee.org/announcements/80211gapp2.html
(7Jun 2003)

[6] KPMG “Survey reveals hackers hunt for wireless networks whilst commuting”.
27 Mar 2003
URL: http://www.kpmg.co.uk/kpmg/uk/press/detail.cfm?pr=1634
(8 Jun 2003)

[7] Netgear. “Wireless Comparison Information”
URL:http://www.netgear.com/pdf_docs/WirelessInforev4.pdf
(7JUN 2003)

[8] Osborne, Mark. “802.11 Security – The Attacks Explained”.
URL: http://www.loud-fat-bloke.co.uk/articles/80211attacks-prt1.pdf
(8 Jun 2003)

[9] Osborne, Mark. “Why I built LOUD-FAT-Bloke”.
URL: http://www.loud-fat-bloke.co.uk/
(8 Jun 2003)

[10] Poulsen, Kevin. “Use a Honeypot, Go to Prison?”. 16 Apr 2003.
URL: http://www.securityfocus.com/news/4004
(8 Jun 2003)

[11] Poulsen, Kevin. “Wi-Fi Honeypots a New Hacker Trap?”.
29 Jul 2002.
URL: http://www.securityfocus.com/news/552
(8 Jun 2003)

[12] Spitzer, Lance. “Honeypots - Definitions and Value of Honeypots”.
29 May 2003
URL: http://www.spitzner.net/honeypots.html
(7 Jun 2003)

[13] Eaton, Dennis. “802.11 Security”.
URL: http://www.intersil.com/data/wp/WP0556.pdf
(8 Jun 2003)

[14] Baird, Robert & Lynn, Mike. “Advanced 802.11b Attack”.
URL:http://www.blackhat.com/html/bh-usa-02/bh-usa-02-speakers.html/#Baird
(8 Jun 2003)