Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)
Practical Assignment version 1.4b option 2
Submitted by: Brian Marino
December 28, 2003

Case Study: Correcting a bad wireless deployment

Abstract

The wireless LAN (WLAN) explosion is in full swing across the globe. The ease of a wireless deployment to extend a network in the office makes it a very attractive and cheap solution. With WLAN's so easy to deploy security is often left out of the design. Lack of security on the wireless network leaves a gaping hole to the wired network where the company's servers and sensitive data reside. As wireless technology becomes more widely used, the potential of a security incident increases with every new deployment.

This paper is on a particular company's WLAN woes and what we did to bring the wireless network up to an acceptable level of risk for the company. We will start with what was originally configured and progress through the solution to correct the troubled WLAN's. I will also be talking about the weakness of WEP and what we did to enhance the security of it.

Introduction

We were called by a company and asked if we could come in and perform an audit on the wireless network. The company had some concerns that they might have some exposure to wired network through the wireless network.

The enterprise is comprised of convenient stores and a casino. The casino is the focal point for the enterprise. All the major servers reside at the casino, so all of the data eventually has to pass through the casino network. They accomplish this by using a SONET ring as the backbone between the different entities of the enterprise. Sites that can not attach to the SONET ring are brought on to the corporate network via a wireless connection using bridges and yagi antennas, which we will not be discussing in this paper. This paper will focus on the casino and convenient stores using the 802.11b standard.

Wireless at the convenient stores

Wireless equipment at the convenient stores consist of a wireless access point, a laptop with a wireless network PCMCIA card and a PDA. Store managers use the laptop to order the product from the warehouse to be delivered to the store. Managers use the PDA to perform inventory on the store.

Wireless at the casino

Wireless equipment at the casino consists of multiple access points, laptops, workstations, kiosks, and PDA's. Wireless technology at the casino serves a number of applications through out the facility such as kiosks for promotional events held at the casino. Casino cashiers have wireless laptops and PDA's they use on the gaming floor to accept money from the patrons who want to apply it to their game play card. Administrative staff uses the wireless network for mobility purposes throughout the facility. There are a few retail shops in the casino that use wireless for ordering product and for performing inventory.

Before

With the initial assessment of the wireless network, we discovered that security was pretty sparse, to say the least. All of the probing, scanning, and sniffing was done with **permission *prior*** to the start of the assessment. We cannot stress the words permission and prior enough.

We will first talk about the convenient stores. Armed with a laptop running Netstumbler (www.netstumbler.com) we were able to pull into the parking lot of every convenient store and see the service set identifier (SSID) of the access points and whether or not they were running encryption. Netstumbler is a free windows utility that is used for auditing 802.11b networks. The default SSID had been changed but there was *NO* encryption at all on any of the access points. That meant that anyone could drive up with a laptop, do very little work and be on the network. Now that we have the SSID and know that there is no encryption on the device, we start to do some recon work.

Using Ethereal (www.ethereal.com) to capture packets we were able to obtain the IP scheme for every location we went to. Ethereal is a free Windows and UNIX based network protocol analyzer which allows you to examine data live from the network or from a capture file. Powerful features such the rich display filter language and the ability to reconstruct a TCP stream make Ethereal a must have tool. After we obtained all of the information needed, we configured our laptop to connect to the network by entering the SSID and an IP address. Voila! We're in.

Once on the network we used a tool called NMAP (www.insecure.org/nmap) to start mapping the **entire** network. NMAP is another free, powerful tool that can map out large networks in very short amount of time. We ran a ping scan against an address range that encompassed the one we had discovered with Ethereal, we hit the mother load. We not only received information about the network that we were connected to, we received information about the networks it was connected to. WOW! Now that we know all of the active IP addresses for the entire enterprise, we can now use NMAP to do TCP/IP fingerprinting to guess remote operating systems and port scans to find vulnerabilities in the systems we have located. There are a lot of other tools we can use to leverage the information we have just gained, but those we will save for a different discussion. It was pretty scary what we had learned about a fairly good size network with approximately forty-five minutes of easy work.

When we entered the stores, more than half of them had laptops out in the open completely unattended. We walked up to one of the laptops and started snooping around. It was already logged into the network for us, making an attack very easy. At one particular store it was about a half hour before an employee asked us what we doing. In case you didn't already know, this is a **BIG** problem. In about thirty seconds an attacker could install a damaging virus or maybe a Trojan to call home to the attacker's computer and start enlisting more of the company's computers to do the same. This was one of the things we addressed pretty quickly (discussed later).

Next, will talk about what we found at the casino. Using the same laptop as before, we sat in the parking lot of the casino and started our assessment. Results were a little different this time, but still not up to par.

Again using Netstumbler we were able to get the SSID and whether or not the access points were encrypted. The access points at the casino are using encryption. There are some tools out there, one being AirSnort (www.airsnort.shmoo.com) that can crack the WEP key. AirSnort is a really cool tool that can be used as a wireless packet sniffer that passively monitors WLAN traffic and computes the encryption key when enough packets have been gathered. We have not yet tried this tool, but it is something that we are aware of (and you should be to) and do plan to try in the near future. Although we were not able to get any data at that time we knew that an attacker that was all set up to do so, could. Just because we could not perform the exploit against WEP does not mean that we didn't do anything to enhance it. There are a lot of things that I can't do that an attacker can.

After we completed the scans of the wireless networks we looked at the actual configurations of the access points. All we had to do to view the configurations on the access points was to open a web browser and enter the IP address. Well, that as pretty easy. At the convenient stores the only configuration changes that were made were that the SSID was changed and an IP address was added. No username and password had been added to any of the devices, that's why we could get in easily. So basically if an intruder were to get on the access point he could then lock everybody out but himself (SCARY!). The casino configurations were a bit different but still not appropriate. Encryption was enabled, but still no username and password.

During

There is no silver bullet to network security. We attended the SANS firewall class, and the instructor said that "You can not build one big wall around your infrastructure to keep intruders out, because they will get in, and the chances of you finding out are greatly reduced, but you can put a lot of little walls up to slow them down and possibly make a mistake so you can catch them" (Chris Brenton). The following are measures we took after the assessment to correct the problems we discovered and mitigate risk. I will discuss the problem or vulnerability and what we did to fix it. All of the configurations ended up being pretty much the same with the exception of the SSID's and encryption keys so I will be referring both locations at the same time.

So we can meet or exceed the expectations of the company, we first conducted interviews with the employees of the company. We spoke with the end users to find out what their needs were. We then spoke with the IT department to get their expectations of what the wireless network should be. Lastly we spoke with the executives of the company to find out what an acceptable level of risk was to the company. Now that we know what is expected of us, we can get to work.

With the level of exposure we were dealing with, we had to quickly implement something until we could get to the some of the higher level solutions.

We started out by putting access control lists on the routers at all of the sites to localize the traffic. Only permitted addresses were allowed to traverse to WAN link back to the casino. Now we knew that someone could spoof a permitted address and gain access, but our thought was, if an intruder did spoof a permitted address we would see an IP conflict and know something was wrong. The access control list was just a quick hitter to get something in place. After we had the access control lists in place we started to really lock the sites down.

The next step was to put MAC address authentication on the access points. MAC addresses are assigned to the network interface card (NIC) and are unique on every NIC. To use this feature simply get the MAC addresses of the stations that are permitted and enter them into the MAC address table on the access point. You must then select **DISALLOW** on all enabled authentication types. That will force all client devices to authenticate using the MAC address of their NIC. MAC addresses are also susceptible to spoofing, but again duplicates will cause problems on a network. All an attacker has to do to spoof a MAC address is, sniff the network traffic to get the MAC address of a legitimate machine, change the universally administered address (UAA) on his NIC to a locally administered address (LAA). MAC addresses that are not in the MAC filter table are blocked from passing traffic through the access point.

The previous steps will only deter a novice hacker. To a higher level hacker with a determination to gain access, they are just minor inconveniences. We must add a few more walls.

The next thing we did was add user names and passwords to the access points for administration purposes. With no user names and passwords on them before any changes that we made an attacker could change them back or change them to lock legitimate users out. We used the local user database on the access point. Although this is not optimal, it is better than nothing.

One thing we implemented might not seem like a security feature but we thought it needed to be addressed. One advantage of the 802.11b radios is the range, but in some cases can be a disadvantage. As previously stated we were running scans from the parking lot. How many security professionals go out and check the parking lot on regular basis for attackers trying to gain access? Chances are, not many. We took notice that we were approximately 150 feet away from the building when performing the scans, in our car. There is a nice little setting in most wireless access points that allows you to adjust the output power of the radio. The access points were set to the default 100mw of output. We adjusted the output down to 5mw which minimized the size of the cell to where the business could still function but an attacker had to be substantially closer, if not in the building to do any type of packet capture. Now that gives us an advantage because it brings the attacker out of the car and into the open where we can see them. That minor

configuration change alone reduced the visibility tremendously. From the standpoint of visibility we also noticed that the access points were out in the open where a potential attacker could see them. An attacker would then know that we are running wireless and what manufacturer's product we use. They could then find specific vulnerabilities against that particular product and exploit them. We decided to have access points moved into security domes in the ceiling effectively hiding them from sight.

Although we adjusted the power output on the access points we still were able to walk into the store with the laptop and sit down at one of the booths and start scanning again. We were never even approached by an employee inquiring as to what we might be doing with a laptop in the store. Not that the employees were to blame, they were never told to be on the lookout for anything like that. We sat down with the security department of the organization and discussed a user training program. The now required user training basically covered what to be on the lookout for. Seeing how there is no free wireless internet access being offered at any of the locations there should be no reason for anyone to be walking around the store with a laptop or PDA. The employees were instructed to ask the patron to discontinue the use of the laptop or PDA or leave the premises immediately if they did not comply, the employees were then instructed to call the security department for further instructions. When the call goes to the organizations security department, they in turn call the IT network security team to start monitoring the location for any potential malicious behavior, even if there is none, the patron is still asked to discontinue use of the device. The security department would then assess the situation and determine whether or not outside services were needed to take care of the situation or if they needed to deploy a security officer the escort the patron off the premises.

Physical security is also important not only to the security of the wireless network but the entire corporation. If a laptop or a PDA were to fall into the hands of an attacker, not only would it be a loss of equipment and the money spent on the equipment, the attacker would now have easy access to the network. How much is your data worth to your company? This particular company's data is very import to them because of the patron's credit card transactions. We needed to institute a policy that would protect the company's equipment and more importantly their data. We told all employees that when the laptops and PDA's were not in use they were to be stored in the managers office at the convenient stores and in the remote cashier closet at the casino, both of which were to locked at all times. Anybody breaking the policy would be subject to disciplinary action.

We will now move on to Wired Equivalent Privacy (WEP) and some of the major vulnerabilities associated with it. WEP was already implemented at the casino, but not at the convenient stores. A newer feature that has come out to help WEP be more secure is Temporal Key Integrity Protocol (TKIP) which provides two major enhancements. The first being Message Integrity Check (MIC) and the second is per-packet keying on WEP encrypted packets.

Let's first talk about WEP. WEP is based on the RC4 stream cipher that was invented by Ron Rivest of RSA Data Security, Inc. which is symmetric key stream cipher. Key stream ciphers work like this, a key stream is generated from the key and then the XOR function is performed with key stream and the plain-text data to get the cipher-text. One vulnerability with this is the Initialization Vector (IV). The IV is used to alter the key stream, its 24 bits long and transmitted in clear text, so anyone sniffing

can see it. So on a 64 bit and 128 bit encryption key the effective key strength is only 40 bits and 104 bits because the IV is not encrypted. Cryptanalyst Fluhrer, Mantin, and Shamir discovered that a WEP key could be derived by passively collecting frames from the network. Initialization Vectors can reveal key bytes after statistical analysis making 40 or 128 bit keys vulnerable and on a busy network the keys can be cracked in a little as 15 minutes. Attackers can accomplish this because again the IV is only a 24 bit field which is about 16.7 million different possible values, WEP eventually will use the same IV for different packets.

WEP is also susceptible to bit-flip attacks because of flawed integrity checking. The integrity checking in WEP is based on CRC-32. CRC-32 is linear and makes it easy to predict the new CRC value when the data is modified. During a bit-flip attack an attacker sniffs the network, captures a frame, randomly flips bits in the data payload of the frame. The attacker would then modify the Integrity Check Value (ICV) of the encrypted payload then retransmit the frame. The receiver gets the modified frame, calculates the ICV based on the frame contents and accepts the packet. The receiver de-encapsulates the frame, processes the layer three packets and because the bits are flipped the checksum fails. The receiving device generates a predictable error that the attacker is sniffing for. When the attacker receives the error message he is able to derive the key stream.

One other problem with WEP is shared secrets. The same shared secrets are on all the hosts that need to access that particular access point. The shared secret is used to encrypt the data and is also used to decrypt the data. Using the same key on all of the systems has some serious drawbacks. One is if an attacker were to compromise a single machine on that wireless network, it would then be able to decrypt all of the data. Another, is rotating keys on a regular basis can be a very difficult and time consuming task.

There is a replacement for WEP and its called Wi-Fi Protected Access (WPA). WPA is a solution developed by the Wi-Fi Alliance that is a subset of the Institute of Electrical and Electronic Engineers (IEEE) 802.11i security specification. WPA uses TKIP and that will be discussed later. In order for WPA to work properly the clients and access points must have WPA enabled for encryption to and from an authentication server that supports Extensible Authentication Protocol (EAP), such as a RADIUS server. Until the user has authenticated to the server it will not be allowed to send traffic to wired network.

Temporal Key Integrity Protocol (TKIP) also known as WEP key hashing, defends attacks against WEP where the unencrypted portion (called the IV) of the WEP frame is use to calculate the WEP key. TKIP removes the predictability of the IV's so the attacker can not calculate the WEP key. TKIP will protect both unicast and broadcast keys alike. If the client device or the access point does not support TKIP they will not be able to use this feature. Some company's added this feature to their products prior to it being ratified. Part of TKIP is Message Integrity Check (MIC). MIC adds a few bytes of data to the packets making them tamper proof. This protects against the bit-flip attack. MIC also adds a sequence number to the wireless frame. Any frame received out of sequence by the access point will be dropped.

With the products the company was using we were able to take advantage of TKIP and MIC because the vendor included them as a pre-ratification enhancements to

WEP. Although it would be much better to follow the WPA security specification that was not an option at this point.

After

Security at the company was enhanced tremendously due to some of the features that come free with most products. Things like MAC authentication, WEP with TKIP, Access control lists, user awareness training, and protecting the configurations of the access points all contributed to enhancements.

After all of the improvements were made, we went back and performed another assessment. The results are starkly different this time around. We pulled into the parking lot of the locations and were not able to pick up the access points this time. We had to get out of the car and walk up to building to even get a weak signal. As we were standing outside one of the buildings with laptop in hand, an employee was coming into work and asked what we were doing? We explained that we were hired by the company to do an assessment of the wireless network. The employee then said that he was not aware of an assessment that was to be taking place and that we would have leave or he would call security. Wow! It worked. Although we were not confronted at all locations, some of the employees actually used the training they were given. I guess the training program needs to be tweaked a little and emphasized more.

After we returned with a security escort we finished our second assessment. We could still get SSID's of the access points but that was about it. We tried sniffing the network but were unsuccessful with our attempts. With MAC authentication enabled, we were blocked from associating and authenticating to the access point and could not get any data from it. Using previous information from the initial scan we tried to scan the IP range again. Again we were unsuccessful with our attempts. With WEP enabled along with the enhancements we could not pass any traffic through the access point.

As you can see there was no one solution to fix the entire problem. MAC address authentication as the only security measure would not be very secure, but when you add WEP it becomes better. WEP has its problems and is not very secure itself but after adding Temporal Key Integrity Protocol and Message Integrity Check it becomes a pretty secure option. Now, adjust the output power so attackers can't sit in their car and attack you from somewhere out of plain view. Teach the employees to watch for potential attackers and take the proper steps to report such problems to the appropriate people. Now we have a security plan that is starting to shape up to be something that can actually keep intruders out. Add user names and passwords to the devices to protect the configurations. Hopefully, with the addition of our smaller security walls we will discourage attackers that can get close enough to access point from moving any further with their attack. We combined multiple solutions and protocols to get the company to an acceptable level of risk determined by the company.

Just because we achieved an acceptable level of security for the company doesn't mean it's over. We need to make sure that the company stays ahead of the curve. We

made some suggestions for future enhancements to the network. One is using WPA or AES encryption instead of WEP. Another would be to use MAC and user authentication on a remote RADIUS server instead of using the local database on the device. The company should think about using VLAN's (Virtual Local Area Network) on the network with IPSec tunnels. These were just suggestions that we had made to the company. Although the previously discussed solutions might not work for every company they worked for this one. The solution also may not be rock solid, but it was at an acceptable level of risk for the company.

Summary

Wireless technology is a great alternative to running wires for temporary connectivity and is also great for productivity within the organization. Realize that there are risks to these great alternatives and try to mitigate the risks as best possible and not using default configurations, you can protect yourself against most attacks. We looked at what one company had for a wireless deployment, assessed the problems and provided some solutions to those problems. Again, as you can you can see, there was not just one solution to the problems faced by this company and that there is no security silver bullet, it takes multiple technologies and protocols to achieve and strong security posture. Every company is different and so is the risk that they are willing to accept, so the solutions provided to this company may not meet the expectations of your company but it worked for them. This particular company had a limited budget to work with for this year and could not do everything suggested but they do have a roadmap to go by for next year and will continue to increase the security of their entire network. The security of the network, wireless and wired will always be under attack, so security professionals must continue to keep themselves abreast of the latest vulnerabilities and exploits to equipment that they are running and patch them appropriately. If your company uses wireless technology you must make sure that it is secure because you are not only vulnerable on the wireless side, you are vulnerable on the wired side.

References

http://www.sans.org

http://www.sans.org/rr/catindex.php?cat_id=68
Wireless LAN: Security Issues and Solutions
Rafidah Abdul Hamid

http://www.sans.org/rr/catindex.php?cat_id=68
Wireless is not the Problem
Jack J. Couch

http://www.sans.org/rr/catindex.php?cat_id=68
Wireless Networks: Security Problems and Solutions
Jonathan Weiss

http://www.cisco.com

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009c8b3.shtml
Cisco SAFE: Wireless LAN Security in Depth
Sean Convery
Darrin Miller
Sri Sundaralingam

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a00800b469f.shtml
A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite

http://www.cisco.com/en/US/products/hw/wireless/ps458/products_configuration_guide_chapter09186a0080107af5.html
Security Setup

www.wi-fiplanet.com

http://www.interlinknetworks.com

Wireless Security
Randall K. Nichols
Panos C. Lekkas

802.11 Wireless Networks The Definitive Guide

Matthew S. Gast

SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs
SANS