Global Information Assurance Certification Paper

Full Name:
Guillermo Antonio Chacón González

Course:
GIAC Security Essentials Certification

Title:
What's new in Standard Wireless IEEE 802.11b

What's new in Standard Wireless IEEE 802.11b

Abstract

This paper is an overview of what IEEE and the manufacturers are doing to make wireless networks more secure. It begins with concepts of Wired Equivalent Protocol (WEP), the eternal flaw and the principal wall in the growth of wireless. This is followed by NetStumbler, this is a tool used to perform attacks and is suggested to help the administrators to make their wireless network more secure in detecting vulnerabilities or attacks like War dialing and ARP attack. Brief description on the ARP attack, New solutions from IEEE and a brief review of the new products from Cisco and 3com which are intended to provide more security. I Selected a paragraph from the University of Maryland about the new protocols used by Cisco. The document ends with some specific tips to make a good deployment of wireless networks such as use of WEP, how is the best place to install the access point, what happen if is configured DHCP, recommendations to use RADIUS as authentication and other else.

Introduction

'People don't believe there's a security problem if you don't prove it to them.' Peter Shipley

The Wireless networks based under standard 802.11, as well known as Wi-Fi, were the innovation last year and promises to be one of the most popular in the 2002. In the companies that use of Pocket Pc and other hand appliances are growing and making more convenient the advantages by cost and productivity of wireless.

New standards at horizon will solve insecurity and interoperation problems which in this moments hold up the development at companies.

In the past year, you've read articles warning about the security holes in wireless networks and documenting the flaws in Wired Equivalent Privacy, the standard method for securing 802.11b wireless LANs. We decided it's time to stop crying wolf and time to test solutions to the problem of 802.11b security.

What to choose?

What to choose is the most difficult decision in the 802.11 implementation. It is not easy to do, 802.11 transmits data up to 11Mbps, this was ratified in 1999. and today it continuous to be the standard in the wireless networks.

But at the beginning of the 2002 new products with support to the 802.11a standard will be introduced in the market. A 802.11a network operate different than operate a 802.11b network and it can provide speed of data transference up to 54 Mbps. The most recent standard in wireless IEEE network is the 802.11g this use the same

frequency than 802.11b, so the products for 802.11b and 802.11g must be interoperated. Furthermore, The standard 802.11g provides a data rates up to 22 Mbps. “Technically, the difference between the two is that 802.11a operates in the 5GHz waveband, while 802.11g operates in the 2.4GHz waveband--where current WLAN products based on the 802.11b standard operate. The final 802.11g standard will probably not be completed until the beginning of 2003”[1].

WEP

The 802.11b standard includes a provision for encryption called WEP (Wired Equivalent Privacy). that in theory makes it difficult to jump onto someone's wireless network without authorization, or to passively eavesdrop on communications. Depending on the manufacturer and the model of the NIC card and access point, there are two levels of WEP commonly available - one based on a 40-bit encryption key and 24-bit Initialization Vector (also called 64-bit encryption and generally considered insecure) and a 104-bit key plus the 24-bit IV (also called 128 bit encryption.)

January 2001, Researchers from University of California at Berkeley print a document revealing a great number of weakness on WEP, this permit to hackers break the sophisticated encryption software, this has been originated a number of press releases talked about this vulnerability. Recently, Scott Fluhrer, Itsik Mantin and Adi Shamir published a paper titled "Weakness in the Key Scheduling Algorithm of RC4". This paper outlined a method for pulling up the master WEP key that would allow a hacker to pose as a legitimate user of the network.

These days, any hacker or script kiddie can use one of several tools, such as WEPCrack or AirSnort; AirSnort, a program that runs on a Linux system with a 2.4 kernel and Prism-based NICS can discover a WEP key after passively monitoring a wireless network. According to the site (http://airsnort.sourceforge.net), AirSnort can determine the WEP key in seconds after "listening" to 100MB-1GB of traffic. And since the current implementation of WEP is based on static keys (that never change over time), eventually you'll ferret out the data you need to crack the key if you listen long enough.

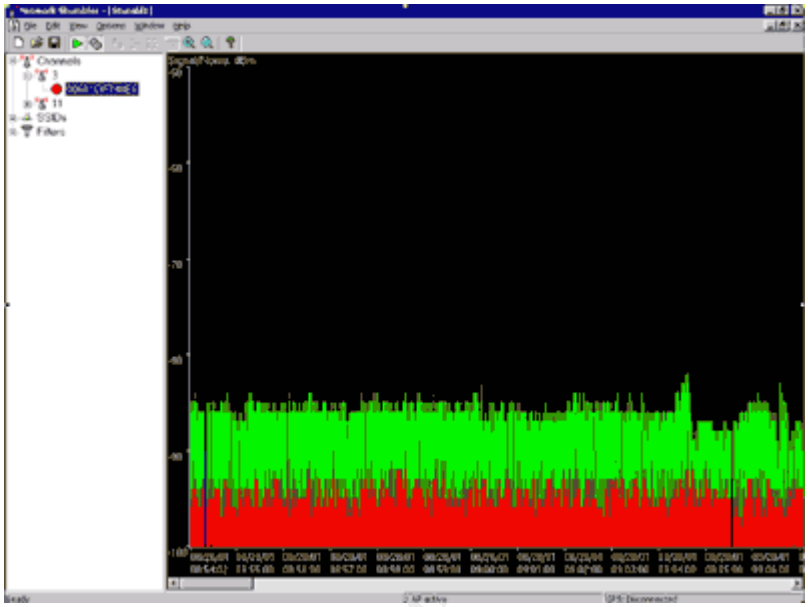
The hacker can load the keys into a wireless network Sniffer same as Wildpacket’s Airopeek or Sniffer technologies sniffer Wireless and gain total access into the data transmission.

NetStumblin' Along

NetStumbler, a shareware program available on www.netstumbler.com, used in conjunction with a Lucent-chipset based Orinoco NIC "sniffs" for wireless networks. The data that NetStumbler returns is truly amazing. When NetStumbler identifies an 802.11b signal, it logs the MAC address of the access point, the network name, SSID, manufacturer, channel that it was heard on, WEP Enabled (Yes or No), signal strength,

[1] Judge, Peter. “Is 802.11g Wireless Doomed?”

signal to noise ratio, and various flags. In addition, if you have a GPS that outputs standard NMEA (National Marine Electronics Association's standards for data communication between marine instruments) data, the latitude and longitude data points are also entered into the log file. Additionally, a real-time display showing signal strength is available.



Many people assume that the 802.11b signals only travel a relatively short distance--maybe a hundred feet or so. They actually travel much farther, but are too weak to be detected by the tiny antennas in laptop cards. But with an external gain antenna, such as a 14dB yagi, 802.11b signals can be detected at a much greater distance.

ARP ATTACK

A hacker could use an attack called ARP (address resolution protocol) poisoning or ARP spoofing to fool computers on the wired portion of the network into sending data to the hacker. The attack creates a fake network address that the network treats as a legitimate destination.

Networks use a table called an ARP cache to match IP addresses to hardware addresses. Data packets coming into a network router ask the ARP program, which is responsible for managing the ARP rules that control the cache, to find a MAC (media access control) address on the cache that matches the packet's IP address so it can be sent to the right machine. If no match is found, the ARP program asks every machine on the network for a match to the IP address, then updates the table if it finds it.

A hacker can exploit ARP by forging data packets from within the network that ask for an IP address which doesn't exist. When the ARP program broadcasts a request for a match to the network, the hacker again forges a positive response from the hacker's computer for the fake IP address. The ARP program then updates the ARP cache table, adding the hacker's computer to the official list of trusted computers on the network.

New Solutions from IEEE

The scope of IEEE's 802.11b Task Group I is "to enhance the 802.11 Medium Access Control to enhance security and authentication mechanisms." One solution is referred to as "generic composition," and combines proven methods for encryption, such as Counter - Advanced Encryption Standard (AES) with proven methods for authentication, such as Cipher Block Chaining. By "authentication" it refers to what Phillip Rogaway of University of California, Davis, calls a "message integrity code" or a "message authentication code." This refers to the process of authenticating each message, not just the user[2].

One of the most promising things to come out of IEEE. Its the consideration of Rogaway's OCB (Offset Codebook), which uses a 128-bit AES block cipher with 128-bit keys to provide for message authentication as well as encryption with a processing overhead instead of use only encryption.

Manufacturers like Cisco, Lucent, 3com and Aguere still supporting the proyect of the standard 802.1x, each of them has been developed proprietary solutions with a similar functionality. Let's take a look to some technology offered

Cisco

Cisco's wireless access point is a sleek, dark-gray box with two flip antennas. Instead of a power jack, Cisco uses a "power injector" that sits between your LAN jack and the access point. To configure the unit via serial port is available to use a serial communications program such as HyperTerminal or Telnet.

Cisco's wireless have three levels of security you wish to use: none, EAP or LEAP.

"None" uses 128-bit fixed WEP keys, it's easily cracked.

EAP was developed to support multiple authentication mechanisms. Instead of selecting a specific authentication mechanism at the link control phase, it waits until the authentication phase. This allows the authenticator to request more information before determining the specific mechanism, and provides a means for an external server to provide the authentication mechanisms, while EAP merely acts as a pass-through. EAP is a complex standard, and its complexity means it isn't widely deployed.

LEAP is Cisco's proprietary lightweight implementation of EAP. It ensures mutual authentication using private and public keys (shared secrets), solving man-in-the-middle attacks, sniffing attacks and active attacks.

LEAP and EAP require a Remote Authentication Dial-In User Service (RADIUS) server. RADIUS enables centralized management of users, and has grown beyond the dial-up

[2] *Rogaway, Phillip, Bellare Mihir, Black Jonh, Krovetz, Ted "OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption"*

stage. By itself RADIUS doesn't offer encryption; it's for authenticating users. You can also configure Access Control Server to perform LEAP and media access control authentication. When combined with the user's logon information and periodic re-authentication, Cisco's LEAP provides the iron-clad wireless security that you need to protect your corporate data, preventing hackers from accessing your wireless LAN, even with a stolen notebook.

3Com

3Com's design looks the best, from its two-position wireless access point with the flip antenna to the retractable X-Jack antenna on its wireless NIC. X-Jack lets you store the antenna in the wireless NIC when not in use, keeping it in your laptop during transportation. Both were a bit over engineered, though. Because the wireless NIC is easily removed from the PC card slot during transportation, that is preferable to having to fiddle with the retractable antenna. If you're at all bumpy with your equipment, you're better off removing the card before moving your laptop anyway.

3Com's Dynamic Security Link technology is similar to Cisco's LEAP. One benefit of Dynamic Security Link is that it increases the number of simultaneous users from 65 to 255. Furthermore, you don't have to manually enter the 128-bit keys when using Dynamic Security Link - it automatically generates new keys and distributes them to the client each session. While this is great for encryption, you'll still need to provide for message and user-authentication for iron-clad security.

The next paragraph was taken textually from the University of Maryland, the author is anonymous. I really like it because, wireless is growing to fast, but today nobody has the key to bring security and this few lines put again the flaw of what wireless is[3].

A current interim solution and why it doesn't work

LEAP is a lightweight EAP installed in the firmware of its cards by CISCO systems. Though it gives a decent solution to many problems it cannot be used because of two major problems.

1. Crypto timing is not possible. Because LEAP is being done in the firmware, it is not possible to enforce rules like key lifetime periods. What is required is a mechanism to enforce crypto periods.

2. Another shortcoming of LEAP is the fact that when authentication takes place it has to take place in the "Open mode"(which uses no WEP). The reason for this is that if authentication is done in an encrypted fashion, a client trying to authenticate for the first time needs to know the current link layer communication (WEP) key. "As our work shows Authenticating in the open mode is very very dangerous".

[3] Author Anonymous. “A current interim solution and why it doesn't work “

3."Disconnected users" are a users in the wireless environment, who have left the network temporarily and as a result of intelligent key management schemes, "do not" have any link layer key which is common with the current set of keys being used in the link layer. Such users cannot authenticate if authentication is to be done in an encrypted fashion.

Keeping your wireless network safe

The follwing poinst are as a result of holes in wireless standard, so it pretend to give some gidelines to portect the network since the beginning of a deployment.

1. Enable WEP. Yes, WEP isn't secure as by now virtually everyone knows, but at least it's a first barrier. And best of all, it's free. Nearly all Wi-Fi certified product ships with basic encryption capabilities. It's just disabled.

2. Change the default SSID of your product. It’s surprised how many access points/wireless routers had the manufacturer's default SSID. that if it still had the manufacturer's default SSID, that the owner probably hadn't bothered to change the default password, either.

3. Don't change the SSID to reflect your company's main names, divisions, or products. It just makes you too easy to target. If your naming is enticing enough, it may attract hackers who are willing to put in the additional effort with tools like AirSnort to break your WEP encryption keys.

4. Don't change the SSID to your street address. Is big the number of SSIDs that used the company's street address. It sure does make it easier to zero in on your location if you broadcast it.

5. If your access point supports it, disable "broadcast SSID". As you take your access point out of the box, broadcast SSID is enabled which means that it will accept any SSID. By disabling that feature, the SSID configured in the client must match the SSID of the access point.

6. Change the default password on your access point or wireless router. Any hacker worth his salt knows the manufacturers' default passwords, and will try them first. Since programs like NetStumbler identify the manufacturer based on the MAC address, it doesn't take much work to figure out what type of device it is even if you do change the SSID.

7. As you do your site survey for access point deployment, think about locating the access points toward the center of your building rather than near the windows. Plan your coverage to radiate out to the windows, but not beyond. If the access points are located near the windows, a stronger signal will be radiated outside your building making it easier for people to find you.

8. As a network administrator, you should periodically survey your site using a tool like NetStumbler to see if any "rogue" access points pop up. All of your hard work to "harden" your wireless network could be wasted if a rogue AP were plugged into you network behind your firewall.

9. Take a notebook equipped with NetStumbler and an external antenna outside your office building and survey what someone parked in your parking lot might "see". You'll be surprised how far the signal radiates. You might only associate at 1-2 Mbps, but it's still a security breach.

10. Many access points allow you to control access based on the MAC address of the NIC attempting to associate with it. If the MAC address of your NIC isn't in the table of the access point, you won't associate with it. And while it's true that there are ways of spoofing a MAC address that's been sniffed out of the air, it takes an additional level of sophistication to spoof a MAC address. The downside of deploying MAC address tables is that if you have a lot of access points, maintaining the tables in each access point could be time consuming. Some higher-end, enterprise-level access points have mechanisms for updating these tables across multiple access points of the same brand.

11. Consider using an additional level of authentication, such as RADIUS, before you permit an association with your access points. While it's not part of the 802.11b standard, a number of companies are optionally including some provision for RADIUS authentication. Orinoco access points, for example, can enforce RADIUS authentication of MAC addresses to an external RADIUS server. Intermec access points include a built-in RADIUS server for up to 128 MAC addresses.

12. If you're deploying a wireless router, think about assigning static IP addresses for your wireless NICs and turn off DHCP. It's true that it's more of an administrative overhead to manage, but a wireless sniffer could easily pick out IP addresses, by not passing them out, it just adds another barrier. It makes it tougher for the casual "drive by" to use your network.

13. If you're using a wireless router and have decided to turn off DHCP, also consider changing the IP subnet. Many wireless routers default to the 192.168.1.0 network and use 192.168.1.1 as the default router. .

14. Don't buy access points or NICs that only support 64-bit WEP. Some low-end products only support 64-bit (40 bit key) WEP, and as you know by now, even 128-bit WEP is universally considered not very secure. Note that some NICs may only require a driver upgrade to attain 128-bit WEP capability.

15. Only purchase access points that have flash able firmware. There are a number of security enhancements that are being developed, and you want to be sure that you can upgrade your access point.

16. Some products support additional security features that are either not defined by the 802.11b standard, or not mandated by the standard. For example Agere Systems' Orinoco access points include a feature called "closed network". This is proprietary, and not part of the 802.11b standard, but if you're in a corporation and deploying one vendor's solution throughout, it really wouldn't matter. With Orinoco's closed network, the AP doesn't broadcast the SSID, so someone using NetStumbler won't see it. The client workstation must be configured with a matching SSID to associate with the AP. The default "ANY" configuration wouldn't associate with a closed network.

17. Most people agree that the best method of securing your wireless network is by using a combination of the suggestions above. However, the most effective strategy would be to put your wireless access points into a DMZ, and have your wireless users tunnel into your network using a VPN. If your corporation doesn't already have a VPN infrastructure in place, it's going to cost you some money to implement. Even if you do have a VPN in place, and all of your clients already have the VPN software, there's going to be an extra effort associated with setting up a VLAN for your DMZ. But this solution adds a layer of encryption and authentication that could make a wireless network suitable for sensitive data[4].

Conclusions

- Security is not a property of a product, it is a property of an environment.
- Information Security is more an issue of governance than it is technology.
- Newer technologies disrupt existing security structures and introduce new classes of vulnerabilities.

Wireless will be growing and becoming in the most popular way to interconnect everything, when all the flaws are repaired maybe our car will be waiting us with the door open and the engine turned on.

My final approach after reviewing some of the flaws of security, is that security goes further than a technological decition we should support our security plan involving CIO and or CISO, and we must ensure that they have this sense of importance. Until then, we are going to be able to support our technology stuff with a security awarness plan and among all the organizations become more efficient, maintaining availability, integrity and confidence of our information

[4] Craig Ellison. "Exploiting and Protecting 802.11b Wireless Networks". September 14th, 2001. PCMagazine.

Strom, David. "Web Informant #268, 30 October 2001: Stealing wireless bandwidth is easy"

Gibbs, Mark. "Less wires, more connections". 10/29/01.

Sources

1) Poulsen, Kevin. “War Driving by the Bay”. Apr 12 2001. http://online.securityfocus.com/news/192

2) Claudia Cooper Church. “Cisco Pioneers Wireless LAN Security”. August 27, 2001. http://newsroom.cisco.com/dlls/ts_082701.html

3) Press Releases 3com. “3Com Announces First Wireless LAN Truly Tailored for Small Business Networks”. http://www.3com.com/corpinfo/en_US/pressbox/press_release.jsp?CLOB_LOCATION=PRESS_RELEASE&INFO_ID=2002450&cntry_cd=US&lang_cd=en-US

4) Author Anonymous. “A current interim solution and why it doesn't work “.Maryland University. http://www.missl.cs.umd.edu/wireless/main.html.

5) Borisov, Nikita; Goldberg, Ian; and Wagner, David.. "Security of the WEP algorithm." May 23, 2001. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (June 10, 2001).

6) Janss, Steve. “ A closer Look at LEAP”. Network World, 12/17/01. http://www.nwfusion.com/reviews/2001/1217revside3.html

7) Sayer Peter. “Wireless LAN Security Fix on Tap From IEEE Group”. Network World, 01/07/02. http://www.nwfusion.com/news/2002/128615_01-07-2002.html

8) Janss Steve. “WEP’s Fatal Flaw Exposed”. Network World, 12/17/01. http://www.nwfusion.com/reviews/2001/1217revside2.html

9) Schwartz Ephraim. “Researchers crack new wireless security spec”. February 14th, 2002. http://staging.infoworld.com/articles/hn/xml/02/02/14/020214hnwifispec.xml?

10) Craig Ellison. “*Exploiting and Protecting 802.11b Wireless Networks”. September 14th, 2001. PCMagazine.*

11) Strom, David. “Web Informant #268, 30 October 2001: Stealing wireless bandwidth is easy”. ***http://www.strom.com/awards/268.html***

12) Gibbs, Mark. “Less wires, more connections”. 10/29/01. http://www.nwfusion.com/columnists/2001/1029gearhead.html

13) *Rogaway, Phillip, Bellare Mihir, Black Jonh, Krovetz, Ted “OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption”. 16/Ago/2001* http://www.cs.ucdavis.edu/~rogaway/ocb/ocb-doc.htm

14) Judge, Peter. “Is 802.11g Wireless Doomed?”. December 19th, 2001. http://www.zdnet.com.au/newstech/communications/story/0,2000024993,20262461,00.htm