Wireless Security, Myth or Reality

Jaya Prasad, Professor *, Indrajit Mukherjee, Systems Manager **

* Department of Computer Science, New Horizon College of Engineering, Bangalore, India
** BE, Computer Science, New Horizon College of Engineering, Bangalore, India,
from.indrajit@gmail.com; ravi8910@gmail.com

Abstract: The rapid growth of wireless network technology and the increasing usage of wireless LANs in various fields promoted the concerns over the security framework available in the existing wireless LAN systems. A wireless LAN is a flexible data communication system using electromagnetic waves for transmission and reception of data over the air. In a typical WLAN configuration, a transmitter/receiver device known as access point connects to the wired network using Ethernet cable. Access point serves as an interface between wireless LAN and the wired network architecture, and acts like a bridge regulating the traffic of data transmission and reception between the wireless LAN and the wired networks. This document provides with the detailed descriptions of the security concerns and flaws that exist and affect the wireless LAN systems and will have a comparative study and analysis of various security suites and protocols that addresses the security issues relevant for the IEEE 802.11 standard series of wireless LAN systems. The paper mostly delves on the preventive steps to be taken before taking a plunge into the wireless world. [The Journal of American Science. 2007;3(2):1-6]. (ISSN: 1545-1003).

Keywords: WLAN; Network Security; Wireless; WEP; Hackers

1.0 Introduction:

With respect to the "secure" wireless technology known as "WiFi," it is entirely possible to deploy a reasonably secure wireless network with 802.11b, but not all WiFi networks are secure. Some, if not most, are woefully insecure. Many weaknesses were discovered in Wired Equivalent Privacy (WEP), the standard security technology deployed with WiFi. Vendors have been working on enhancing the security of wireless networks, and we are just now beginning to see the fruits of their labors. Technologies such as WPA (WiFi Protected Access) solutions are currently shipping, and 802.11i is just around the corner. Both these protocols will enhance cross-vendor support for wireless security But to say that WiFi is secure is a bit of a leap. Time and time again, the market has discovered that proprietary security solutions are frequently inadequate. It is considered a "best common practice" to use security protections that have undergone third party or open scrutiny.

1.1 The Present Problem:

The problems with proprietary solutions are somewhat subtle. It seems a prudent precaution to not tell potential hackers what security measures you've put in place. But the primary problem with proprietary security systems is that as a system designer, one must foresee all possible situations in which a product or technology would be used, and how that affects system integrity. An attacker, on the other hand, must only find a single vulnerability to prove your system insecure. Peer and third-party review of open systems is considered the best practice when developing security components. The idea is to present your plans to your peers, who role-play being attackers. If the only attacks your peers can find are ones whose risks can be mitigated by physical or procedural security measures, then you may have adequate protection.

But this is still not a guarantee that a system which is secure today will remain secure in the future. Modern security development practice calls for security features that can be easily replaced should they be found to be vulnerable. Whit Diffie, the inventor of public key cryptography, explains this eloquently in his online essay, Decrypting the Secrets to Strong Security.

2.0 Truths about Wi-Fi Security:

We are pleased to hear that vote data is not transmitted across what could be an insecure network, but without more knowledge of the system it is hard to say that the AVS solution includes adequate protections for even the "non-sensitive" information that is used to configure and track the voting machines. We couldn't help but wonder, if the system designers used any form of security in their wireless protocols, doesn't that mean they believed there was some risk to allowing the information to be transmitted unprotected?

As a closing note, we wish to stress that we have no proof that most of existing security systems are insecure. It is certainly possible that their products may possess superior security. The problem is we have no way of knowing.

Wireless networking has been an issue of security since its creation. With early technology it was simple to steal someone's data or connect into their LAN. Some advances were made, such as encryption and the need for MAC (media access control) addresses on the access point, but it was still relatively simple to bypass these security methods. New solutions in wireless networking security such as CCE, WPA, and AES are helping to destroy misconceptions and improve security.

The first real standard for wireless security was WEP (Wired Equivalent Protection). It did not live up to its name. WEP offered only basic security. Free utilities available online can be used to find wireless networks and attempt to gain access, such as AirSnort. Its simplicity to crack comes from the use of a static 40 or 128 bit encryption key. This key had to be entered manually on every device wanted to communicate with the WLAN (Wireless Local Area Network).

2.1.1 Encryption Facts:

WEP encrypts your data so that no one can read it unless they have the key. That's the theory behind WEP, anyway. WEP has been a part of Wi-Fi networks from the beginning. (The developers of Wi-Fi were initially focused on the business market, where data security has always been a big priority). The name itself belies the intentions of the system's developers; they wanted to make wireless networks as secure as wired networks. In order for WEP to work, you must activate WEP on all the Wi-Fi devices in your network via the client software or configuration program that came with the hardware. And every device on your network must use the same WEP key to gain access to the network. (We talk a bit more about how to turn on WEP in the "Clamping Down on Your Wireless Home Network's Security" section of For the most part, WEP is WEP is WEP. In other words, it doesn't matter which vendor made your access point or which vendor made your laptop's PC card network adapter — the implementation of WEP is standardized across vendors. Keep this one difference in mind, however: WEP key length. Encryption keys are categorized by the number of bits (1s or 0s) used to create the key. Most Wi-Fi equipment these days use some System for Securing Wireless Networks.

2.1.2 Security Requirements:

This paper talks about the design of a secure wireless network. The designers wanted to create a wireless network that: ran under Windows 95 or NT, is compatible with the Raylink WLAN product, uses Fortezza cryptographic PCMCIA cards, provides communication between wireless hosts using Fortezza cards and wired hosts not using Fortezza cards, compatible with all Windows applications, transparent, and have minimal impact on communication performance.

To design this system the group had to determine which level they were going to use to encrypt and decrypt packets. The group decided to use the LSP (Layered Service Provide) level. They did not use the data link level because it would have had to modify the WLAN interface driver on the interface card of all users and when drivers were updated they would have to be modified for everyone. They decided not to use the IP or TCP levels because they did not have access to the protocol source code used by Microsoft. The LSP level is below the WinSock-- an application programming interface that lets a Windows program send data over any network transport protocol-- and above the transport layer.

Wireless LANs are popping up here, there and everywhere. Many businesses are implementing wireless LAN segments on their internal LANs because it is easy to setup and obviously there are no wires to run. Wireless allows users with laptops and other mobile devices to roam the enterprise and not have to plug in wherever they go. As part of the process of implementing a wireless network segment on the corporate LAN of the company that I presently work for, I did some research and testing of wireless security. Too often people think that because the setup of a wireless segment is literally plug and go that everything is functioning properly and securely. Wireless is a virtual playground for hackers, the technology is still quite new.

3.0 Technical Paradigms:

3.1 Security Concerns:

It shouldn't be so much of a surprise that 802.11b networks have taken off to the degree that they have. The combination of relatively high speed, low price, and ease of installation make them an "instant hit." There is a dark side to 802.11b though, in the latter half of 2002 WiFi security has become the conversation topic of choice at corporate IT water fountains and coffee machines. By now, just about everyone has heard of problems with WiFi security. At first it was a theoretical problem detected in a review by a team of UC Berkeley grad students. WiFi device manufacturers and the IEEE (who devised the original 802.11b security protocol called WEP) downplayed the vulnerability. No-one wanted to admit the awful truth: the 802.11b Wired Equivalent Privacy protocol was seriously and fundamentally flawed. But by this time it was too late; tens of thousands of 802.11b systems had already been shipped; an army of unix hackers pieced together tools to pierce the anemic security offered by WEP. Meanwhile, the academic community released a stream of additional weaknesses.

3.2 Technology Comparators:

The IEEE and device manufacturers have announced updated security protocols that should not suffer from the same vulnerabilities, but consumers and corporate IT staffs will have to wait for devices based on new standards to be designed, tested, and shipped. Where does this leave the wireless community? We're not out of the woods with respect to security, but it could be worse. WPA (WiFi Protected Access) will be a definite improvement over WEP, but it will be several months before WPA enabled products are available in the channel. 802.11i is a distant solution promising improved security over WPA, but it is at least a year away. Most vendors and analysts believe that 802.11i will require new hardware. And both WPA and 802.11i based products will come with a WEP reverse-compatible mode that would most likely defeat any security improvements if it is used.

4.0 What do we do about it:

4.1 Security Proposals:

This document is intended for users of existing heterogeneous 802.11b networks. It is intended to be a concise list of steps you can take to limit the security risk of operating an 802.11b network. This checklist is not all-inclusive, and as always, some features listed here may not be practical (or even possible) with your network hardware. You mileage may vary, but this list is a good start for those home and corporate users interested in getting a good start towards securing their wireless network.

4.1.1 Check for perpetual security upgrades:

Some WiFi product vendors have included proprietary enhanced security features. A notable example of this is the Cisco Aironet 340 family which contains a number of security enhancements over WEP. The drawback is that in order to benefit from proprietary security enhancements, one must generally operate a homogeneous wireless network with hardware from only one vendor. For users that have not yet deployed a wireless network, this may be an option worth investigating.

Note that proprietary enhancements that only increase the length of the WEP key are mostly valueless. WEP has been shown to be "unsafe at any length." A 128 bit WEP key is only marginally more secure than a 64 or even 40 bit WEP key. Note that some proprietary enhancements are delivered along with longer keys. It is the unfortunate truth that the marketing departments of some of these vendors only mention the longer key length or mention it as the primary security enhancement. In cases such as this, simply ignore the WEP key length and evaluate the product based on other security features.

4.1.2 Modify your SSID or turn off SSID Beacon PDUs:

The SSID (Service Set ID) is used to identify a family of wireless clients to a wireless or wired gateway. Not surprisingly, most (if not all) wireless devices from the same manufacturer ship with the same default SSID. Knowing the SSID is the first step in "associating" a wireless client with a wireless access point. Since an attacker will have to know your SSID to complete the 802.11b protocol to start accessing your network, it's a good idea to make it difficult for an attacker to scan for or guess your SSID. Replace the default SSID in your wireless network with a difficult to guess (preferably random) string. Certain wireless access points can be configured to disable "beacon" broadcasts. In 802.11b terminology, a beacon is a type of packet that contains the SSID of a network. It is used to synchronize the clocks on client devices and to make it easy for new network clients to see what networks are available in multi-networked environments. If you have only one WiFi network that you're dealing with, you can probably live without the beacon. If it's easy to turn off beacon broadcasts, do so.

Sophisticated network attackers will be able to intercept all wireless traffic and sort through packets (even encrypted packets) to find your SSID, so you shouldn't think that just because you don't use the default that it's impossible for an adversary to guess it. Also, it should be noted that very sophisticated attackers don't even need the SSID to eavesdrop on wireless network transactions, so protecting your SSID is certainly not the be-all, end-all answer to WiFi security.

Changing your SSID is a very good beginning, however. At the very least, it will minimize the likelihood that your wireless clients will accidentally connect to your neighbor's network.

4.1.3 Switch on MAC Address Access Control Lists:

Some wireless access points allow network administrators to limit access to the network to a explicit list of network cards. This is usually done at the "MAC address level." The MAC, or Media Access Controller, is simply a fancy name for the wireless card. The MAC address is a 48 bit value that is (supposedly) unique for each network card on the planet. When a MAC Address ACL (Access Control List) is used, the access point will refuse to talk to any wireless card whose MAC Address is not on the list. If you frequently have friends or coworkers over who want to use your network, this feature may be more trouble than it's worth. Also, not all access points support MAC ACLs, but if you have one that does and you have a small number of machines that access your network, consider using this feature.

In the end, however, MAC Address ACLs do not provide ultimate security. The MAC Address is broadcast as part of the normal operation of a 802.11b network, and sophisticated attackers can easily snatch a valid MAC address out of the air, and many wireless cards have programmable MAC Addresses. It's therefore pretty easy for an attacker to listen to your network for a short while, listen for a valid MAC Address, then reprogram his wireless network card to use this valid MAC Address. However, If two machines try to use the same MAC address at the same time, the network may start acting erratically. So, if your network is acting erratically, it may mean you're under attack. Sophisticated adversaries who have the skill to intercept your MAC addresses will probably know that using a MAC address they've sniffed off your network will clue you in to the fact that they're there, so in general, MAC Address sniffing adversaries will wait until they see the machine whose MAC Address they've sniffed disassociate from the network before trying to use it.

Another reason to use MAC Address ACLs is that it is virtually impossible to "accidentally" steal someone else's MAC Address. If an attacker breaks into your network and you are able somehow to learn who the attacker is. It would be difficult for the attacker to claim that he was doing anything other than trying to break into your network if it can be shown that he (or she) sniffed a MAC Address, waited for it to disassociate from the network, then reprogrammed his/her network card to use the sniffed MAC Address.

4.1.4 Run WEP:

Despite the fact that WEP provides virtually no protection from a determined and reasonably sophisticated adversary, it may protect from casual war drivers. In many cases, network attackers are simply looking for free bandwidth. If there are two networks available to such an adversary: your WEP protected network and a second unprotected network, chances are they won't go to the trouble of cracking your WEP keys just to get free bandwidth.

On the other hand, if your network houses sensitive information (super-secret marketing plans, technical diagrams of next year's hot electronic toy, etc.) you should not trust in WEP alone. Reasonably sophisticated adversaries who know (or just suspect) your network contains valuable resources will not thwarted by WEP.

4.1.5 Discourage DHCP . Use DHCP with authorized MAC addresses:

Once an attacker associates with the network, the next step is to establish an IP address. It is probably best to use fixed IP addresses, and not to use DHCP. However, DHCP is becoming indispensable and many network administrators will refuse to part with it's benefits. That's probably okay if it is possible to limit DHCP leases to machines that have associated from an authorized MAC Address.

4.1.6 Employ a Static ARP table:

ARP (Address Resolution Protocol) is the part of the TCP/IP family of protocols that binds MAC Addresses (48 bit unique IDs) with IP Addresses (the more familiar w.x.y.z form addresses.) A type of attack called ARP Cache Poisoning can allow an adversary to intercept just about any transmission on the network. Using a static ARP Cache can prevent this attack, but your access point will have to have explicit support for static ARP tables. Using a static ARP Cache with Static IP addresses simplifies administration somewhat, so don't be surprised if it is difficult to get DHCP to work on wireless access points that allow for static ARP tables.

4.1.7 Commision your Wireless Access Point outside your firewall:

One would think that with all the publicized vulnerabilities of 802.11b networks and all the trade press coverage of Wardriving and Warchalking that no-one would put a wireless access point inside a corporate firewall. Well... there are still several people that don't know that this is a no-no, so if you see someone doing this, you should point him or her to this checklist.

The problem with putting your access point on the inside of your firewall is that heterogeneous 802.11b network security mechanisms are insufficient to defend against even moderately sophisticated adversaries. If you put an 802.11b network on the inside of your firewall, it will be simply a matter of time before someone breaks in.

The standard technique is to put wireless access points on the outside of the firewall and use a VPN (Virtual Private Network) to tunnel through the firewall. VPN software provides cryptographic privacy protections and strong authentication to defend against spoofing, replay, and eavesdropping attacks.

4.1.8 Provide LightWeight firewall software to your wireless users:

Placing your wireless network outside your firewall defends your corporate network, but not your wireless clients. It is still possible that clients on a wireless network can be attacked. If an attack is successful against a legitimate wireless client, a sophisticated adversary could use that legitimate client as the starting point for an attack against the sensitive systems inside your firewall.

It is generally a good idea then to provide "personal firewalls" for wireless client machines. Several products from Network Associates and Symantec can "harden" your typical Windows or Macintosh client. Linux or other Unix clients have a plethora of firewall choices to select from.

4.2 The Bottomline:

Wireless LANs are popping up here, there and everywhere. Many businesses are implementing wireless LAN segments on their internal LANs because it is easy to setup and obviously there are no wires to run. Wireless allows users with laptops and other mobile devices to roam the enterprise and not have to plug in wherever they go. As part of the process of implementing a wireless network segment on the corporate LAN of the company that I presently work for, I did some research and testing of wireless security. Too often people think that because the setup of a wireless segment is literally plug and go that everything is functioning properly and securely. Wireless is a virtual playground for hackers, the technology is still quite new.

Correspondence to:
Indrajit Mukherjee, BE, Comp. Sc.
Systems Manager, NHCE, India
Email: from.indrajit@gmail.com

Received: 5/16/2007

References

1. Mukherjee I. Design Methodologies For Bit Distributed Computer Resource System Advances In Modelling & Analysis, Paris, 1994.
2. Mukherjee I. Design of a Concentrator Based Network Int. Educomp, Chandigarh ,TTI, 1995.
3. Design and Development of a Software lock system" CTCSIS Int. Conference, Amman, Jordan , 1996.
4. Mukherjee I. Introduction to PC Softwares - Academic India Publishers, New Delhi,1995.
5. Mukherjee I. Chapter on I.C.G. in Elements of Computer Science IEEE (AMIE) Narosa House Publn., 1996.
6. Mukherjee I. Beginner's Assembly Language & Hardware for the IBM PC Series, New Central Book Agencies, Calcutta, 1998.
7. Mukherjee I. Even the Dial-up Internet Users , temp. IP Address Owners Deserve an FQDN Address, The Journal of American Science, 2(1), 2006.
8. Mukherjee I. A practical approach to inexpensively link distributed facilities of New Horizon College of Engineering for Data Communication. The Journal of American Science. 2006;2(4):49-52. http://www.americanscience.org/journals/am-sci/0204.
9. Mukherjee. I Suggestions for an extended set of functions to the Point-to-Point protocol, Anveshna, NHCE, Feb' 2007