Global Information Assurance Certification Paper

Is Your Wireless Network Secure?

Ken Hodges
September 10, 2001

Abstract

The use of wireless technology has become increasingly popular due to its flexibility and recent affordability over traditional methods to access hard-wired LANs. This convenience, however, may not be worth the potential for losses incurred by its use. The 802.11b standard has been coming under increased scrutiny in light of a recently published paper outlining a significant vulnerability found with the Wired Equivalent Privacy (WEP) used to secure traffic between wireless devices. Unfortunately, this recent discovery is the latest in an increasingly long list of security issues surrounding 802.11b.

This paper will present the issues surrounding newly discovered vulnerabilities with WEP, as well as current access control problems that exist with the wireless architecture currently in use. It will also propose methods that can be used to help secure wireless LANs.

Introduction

Wireless connectivity offers a freedom and flexibility never before encountered with home and business users. Traditionally, adding users to a network required wiring to be pulled throughout a building and installed by either a hired professional, or an unfortunate network administrator who had been given the task and a crimping tool. On the other hand, with wireless technology, data travels through the air, allowing a user the ability to connect in locations once deemed impossible, or at the very least inconvenient, to the typical hard-wired user. This newly found freedom, though, has come with a price.

Serious security concerns over 802.11b and WEP have been uncovered that have required a moment of pause for those responsible for such wireless installations to determine if the security of a wireless LAN could potentially be sacrificed for the sake of convenience. These concerns, though, don't seem to be deterring the sales or popularity of 802.11b, as the number of wireless devices is expected to grow from 2.6 million in 2000 to 11.8 million by 2003 [LAW].

Weakness of WEP

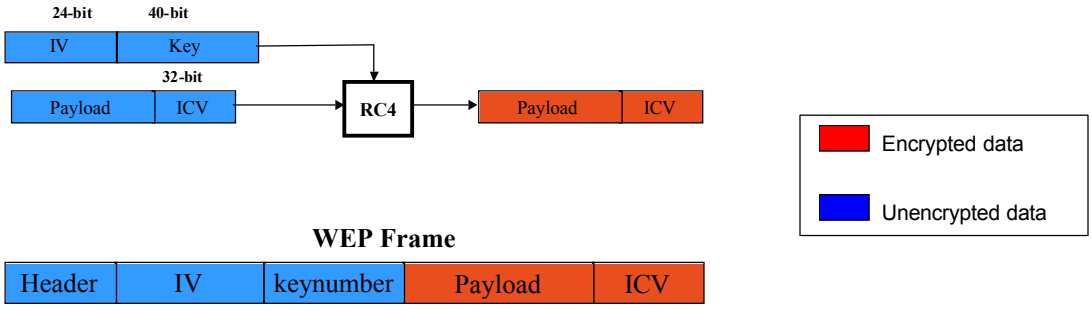
Wireless technology uses Wired Equivalent Privacy (WEP) as a method of encrypting and decrypting wireless communications typically between a client and an access point connected to a wired LAN. WEP depends on the use of a secret key to encrypt and decrypt packets traveling between the wireless

network card and access point. This encryption and decryption takes place using the Ron's Code 4 (RC4) algorithm, which was designed in 1987, and kept secret until it was anonymously posted in 1994 [FLU]. The following is a brief overview of the process of WEP to use as a foundation of recently discovered vulnerabilities.

The process of encrypting an 802.11 frame is essentially a 3 step process. For the purpose of this discussion, we will assume the use of a 40-bit key. In the first step, WEP computes a 32-bit cyclical redundancy check (ICV) on the payload of the frame and appends it to the end of the frame. Next, one of potentially up to four keys, which are all shared between Wireless LAN (WLAN) members, is selected and appended to a 24-bit initialization vector (IV).

One of the problems with WEP is the use (or misuse) of the IV. Typically, the IV selected by the wireless NIC starts at some pre-determined number (such as 0) and incremented by one for each packet that is transmitted [ARB]. One problem is that each time a card is re-initialized, the IV is reset to the starting number, leaving the possibility of low numbered IV to be re-used more frequently [ARB].

Using the data frame+ICV, and the secret key+IV, the message gets encrypted using the RC4 algorithm. This is accomplished by creating a keystream using the secret key+IV and XORing the keystream with the data payload. The frame that is sent is the resulting ciphertext and the IV. It should be noted for clarity that the IV, in addition to the header and keynumber, is sent in the unencrypted portion of the frame. The receiving station uses the sent IV and the shared secret key to decrypt the ciphertext, again using RC4 to accomplish this.



Example of WEP encryption and format of WEP frame [NEW]

Serious problems surrounding the use of wireless LANs and specifically WEP have come to light recently. Researchers from UC Berkeley and Zero-Knowledge Systems released a paper outlining the vulnerability of keystream reuse attributed to mismanagement of IV. It was noted that all possible IV could be exhausted in as little as 5 hours [BO2]. This would allow the potential for an attacker to capture two encrypted packets using the same keystream. This flaw could allow an attacker to not only decrypt the contents of an encrypted packet,

it could also allow an attacker to insert or change traffic, redirect decrypted traffic to an alternate IP address, or even enable an attacker to develop an IV dictionary to use to decrypt any and all traffic traveling within a wireless network [BO1].

In response to the Berkeley/Zero paper, the Wireless Ethernet Compatibility Alliance (WECA) issued a statement that left many in the security and technology field scratching their heads. The WECA is a consortium of wireless vendors whose goal is to promote compatibility of 802.11 and certify interoperability of wireless products. In essence, the WECA countered, "The goal of WEP is to provide an equivalent level of privacy as is ordinarily present in an unsecured LAN…It is important to emphasize that WEP was never intended to be a complete end-to-end security solution [WIR]." Stephan Somogyi commented that the response "spent more time focusing on semantic quibbles and how hard it is to perform the attacks than admitting there were fundamental flaws in the protocol in the first place [SOM]." At the time however, the WECA had a valid point: to mount such an attack was not a trivial process. It required significant time and computing resources to accomplish. Unfortunately for the WECA and 802.11 users, it was only a matter of time before this fundamental flaw became trivial to exploit.

The final nail in the WEP coffin was driven by a recently published paper "Weaknesses in the Key Scheduling Algorithm of RC4" by Fluhrer, Mantin and Shamir. The paper exposed, in complex mathematical detail, two significant weaknesses of RC4 in the Key Scheduling Algorithm (KSA). The first is related to the KSA output where the researchers found that a small portion of the secret key determines a large portion of the initial KSA output. In addition, they also found an inherent flaw used by WEP whereby the secret key can be easily derived by looking at the keystream used with multiple IV. It was originally thought that the main "Achilles heel" of WEP centered around the relatively small IV size (24-bits). The authors make a startling discovery that this newly discovered vulnerability is present not only in the current implementation of WEP but in a future implementation, WEP2. It was found the both the key and IV size made little difference in the time required to compromise the key, and the difficulty of the attack is linear as opposed to exponential in relation to the key length [FIS].

As mentioned previously, the method outlined in the paper to recover the secret key is highly technical and the authors pointed out that no attacks were actually mounted against an actual WEP connection, nor did they claim that WEP may actually be susceptible to this particular attack. It wasn't long, though, before the concept was turned into a credible threat.

Researchers from Rice University and AT&T labs put the theory into practice by cracking encrypted packets, and successfully demonstrating the severity of the flaw. While the researchers did not release the code necessary to mount the

attack, it wasn't long before others did. Two programs are currently available that exploit the recently exposed RC4 vulnerability – AirSnort, and WEPCrack (sourceforge.net). Both programs run under Linux, and require a relatively small amount of captured data: anywhere from 100MB-1GB. After capturing the required data, AirSnort is capable, according to the author, of guessing the password in less than 1 second.

Access Control Problems

As if the problems surrounding WEP were not enough, numerous additional flaws were discovered regarding the way wireless LANs allow access to connected clients. Researchers at the University of Maryland exposed numerous problems with access control mechanisms used by popular access points and PCMCIA 802.11b network cards [ARB].

Typically, an access point has one or several methods available to control access to a wireless LAN. They can include, use of a common Service Set Identifier (SSID), allow access based on MAC address, and as explained previously, WEP.

One common method that is used and has been demonstrated to be extremely insecure is the use of "closed network" access control, whereby access to the wireless LAN is controlled by the use of an SSID or network name. Only clients who know the network name are allowed to join the wireless LAN. Since on many vendor's hardware, the use of WEP is optional, the only thing preventing access to the network is the knowledge of the SSID.

Ruth Cowell wrote about the latest craze "war driving," where the SSID for wireless networks can be quickly found using free and easily obtained software such as Network Stumbler. It was found that during a drive through San Francisco using such software, more than 40 wireless networks were found to have WEP disabled and using only the SSID for access control [COW]. This vulnerability makes these networks susceptible to the "parking lot attack," where an attacker has the ability to gain access to the target network a safe distance from the building's perimeter [ARB].

Still another method used by wireless vendors is the use of allowing access based on the MAC address of the 802.11b network card. The list of authorized MAC addresses allowed on the LAN are stored and maintained in the access points. There are several problems associated with this mode of access control. One being, this method authenticates the equipment, not necessarily the user, onto the network. If an authorized card was stolen, an attacker would have no resistance to gain access to a wireless LAN, assuming there were no other access controls in place. University of Maryland researchers contend that this is also not a reliable method to secure a wireless network, because legitimate MAC addresses can be easily captured by an attacker using a packet sniffer

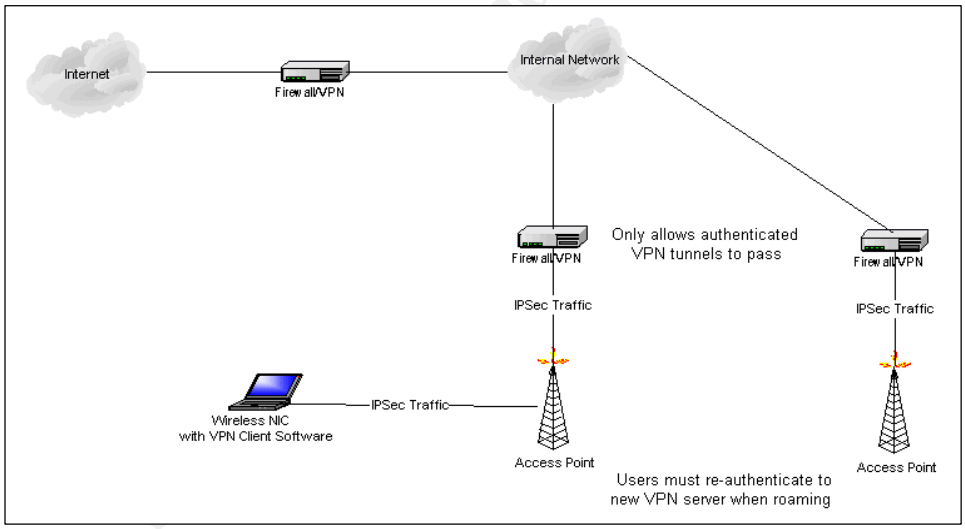
[ARB]. The attacker, they maintain, can then alter the MAC address of their card to gain access. In fairness though, while changing the MAC address of a network card is entirely possible, it is an extremely difficult process, which requires re-flashing the memory on the card, and is therefore not a trivial task to accomplish [CIS].

Is 802.11b Usable?

Is it possible, given all the exposed flaws, to safely use a wireless network? A practice of "defense in depth" is required to ensure that the potential for compromise is minimal. Off-the-shelf 802.11b hardware has been thoroughly demonstrated to be insecure. It is therefore prudent for users to combine several access control methods, to ensure integrity, availability, and confidentiality of the wireless LAN.

VPN's and Secure LAN (SLAN)

The idea behind using a VPN over a wireless link is that packets going to and from an access point will be secure using a much stronger level of encryption, such as IPSEC. In addition, access to the wired network can be controlled with a more robust method of authentication with a VPN server.



Example of Wireless Network Using VPN [AND]

In addition, specialized "VPN" open source software is currently being developed to allow Authorization, Authentication and Accountability for insecure networks such as 802.11b (slan.sourceforge.net). SLAN's are "similar to a VPN and provides server authentication, client authentication, data privacy, and integrity using per session and per user short life keys [AND]."

Remote Access Dial-in User Service (RADIUS)

Several 802.11 access points offer RADIUS authentication, where clients gain access to the network by supplying a username and password to a separate server. This information is securely sent over the network eliminating the possibility of passive snooping.

Dynamic Keys

To reduce the possibility of key compromise, several vendors, including Cisco and Agere, are offering products that eliminate the use of static keys, and instead are implementing per-user/per-session keys combined with RADIUS authentication. Clients must authenticate with a RADIUS server using network credentials, and WEP keys are dynamically distributed securely to the client.

There are several advantages to this method of key distribution. Dynamic keys offer less administrative overhead, since keys are automatically changed with each user logon. In addition, dynamic keys eliminate the vulnerabilities described earlier with using WEP and static keys.

One drawback to this method exists, as there currently is no standard for key distribution in the IEEE 802.11b standard [HAA]. Hence, interoperability is impossible since each distribution method is vendor specific. This hopefully will change later next year with the introduction of 802.11x, which standardizes key distribution and authorization using RADIUS or Kerberos.

Rogue Access Points

As if worrying about how to secure a wireless LAN wasn't enough, IT departments must also deal with employees installing unauthorized access points on the LAN. A recent Gartner survey discovered that "though 20 percent of corporate IT departments believe they have wireless LANs, 50 percent of the procurement departments have said they have bought them [LAW]." This presents a difficult situation for departments in charge of network security. How are you to secure a device you don't even have knowledge of? Fortunately, wireless sniffing software is available on the market today that can be used to easily find rogue access points on a LAN. These can include AiroPeek from WildPackets, MobileManager from Wavelink, Sniffer Wireless from Network Associates, and Network Stumbler from Marius Milner.

Conclusion

The fact is: wireless is not going away. It has become more affordable, and easier to implement than ever before and as such, its use will continue to grow. It is important however to understand what security problems exist with current 802.11 technology, and what is involved with building and maintaining a secure wireless LAN.

With all the vulnerabilities that have been uncovered, it seems clear that the use of 802.11 technology is a double-edged sword. Wireless LANs can be extremely useful, but must be coupled with one or more additional security measures to ensure the most minimal risk of compromise.

Unfortunately, the relative complexity and associated costs with incorporating a secure wireless LAN may leave many home and small business users behind and vulnerable to the attacks outlined above. It may be prudent for some to wait until future enhancements of wireless technology are released and proven to be secure before the benefits are realized.

References

[AND] Andress, Mandy. *Wireless LAN Security*. http://www.blackhat.com/presentations/bh-usa-01/MandyAndress/bh-usa-01-Mandy-Andress.ppt, Black Hat Briefings, August 2001.

[ARB] Arbaugh, William A.; Shankar, Narendar; and Wan, Y.C. Justin. *Your Wireless Network has No Clothes*. http://www.cs.umd.edu/~waa/wireless.pdf, Department of Computer Science, University of Maryland. March 30, 2001.

[BO1] Borisov, Nikita; Goldberg, Ian; and Wagner, David. *Intercepting Mobile Communications: The Insecurity of 802.11.* http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf, University of California at Berkeley, January 2001.

[BO2] Borisov, Nikita; Goldberg, Ian; and Wagner, David. *Security of the WEP Algorithm.* http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html, University of California at Berkeley, February 2001.

[CIS] Cisco Systems. *Cisco Aironet Security solution provides Dynamic WEP to Address Researcher' Concerns.* http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1281_pp.htm, September 6, 2001.

[COW] Cowell, Ruth. *War Dialing and War Driving: An Overview.* http://www.sans.org/infosecFAQ/wireless/war.htm, June 11, 2001.

[FIS] Fisher, Dennis. *Flaws found in key wireless protocol.* http://www.zdnet.com/eweek/stories/general/0%2C11011%2C2802134%2C00.html, ZDNet, August 7, 2001.

[FLU] Fluhrer, Scott; Mantin, Itsik; and Shamir, Adi. *Weaknesses in the Key Scheduling Algorithm of RC4.* http://www.eyetap.org/~rguerra/toronto2001/rc4_ksaproc.pdf, August 2001.

[HAA] Haagh, Jan. *Wireless Network Security Bulletin.* ftp://ftp.orinocowireless.com/pub/docs/IEEE/BULLETIN/SALES/ORiNOCO%20security%20paper%20v1_2.pdf, April 5, 2001.

[LAW] Lawton, George. *Lock up your wireless LAN.* http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2806945-1,00.html, ZDNet, August 23,2001.

[MEH] Mehta, Princy C. *Wired Equivalent Privacy Vulnerability.* http://www.sans.org/infosecFAQ/wireless/equiv.htm, April 4, 2001.

[NEW] Newsham, Tim. *Cracking WEP Keys*. http://www.blackhat.com/presentations/bh-usa-01/TimNewsham/bh-usa-01-Tim-Newsham.ppt, Black Hat Briefings, August 2001.

[SIE] Sieberg, Daniel. *"Off-the-shelf" hack breaks wireless encryption.* http://www.cnn.com/2001/TECH/ptech/08/10/wireless.hack/index.html, CNN, August 11, 2001.

[SOM] Somogyi, Stephan. *802.11 and swiss cheese.* http://www.zdnet.com/zdnn/stories/comment/0,5859,2707262,00.html, ZDNet, April 12, 2001.

[WIR] *802.11b Wired Equivalent Privacy (WEP) Security.* http://www.wirelessethernet.org/pdf/Wi-FiWEPSecurity.pdf, Wired Compatibility Ethernet Alliance, February 19, 2001.