Interested in learning more about security?

SANS Institute InfoSec Reading Room

Perils and Fixes for 802.11 WLANs in SOHOs

Wireless networks, especially 802.11b, are becoming very popular for homes and small offices, despite serious security problems that have been widely reported. We give an overview of the 802.11 standards, the WEP algorithm and RC4 encryption. Then we analyze the various 802.11 security problems and discuss various ways to improve SOHO wireless security.

Perils and Fixes for 802.11 WLANs in SOHOs

Allan Moluf

March 06, 2002

GSEC Practical v 1.3

Abstract

Wireless networks, especially 802.11b, are becoming very popular for homes and small offices, despite serious security problems that have been widely reported. We give an overview of the 802.11 standards, the WEP algorithm and RC4 encryption. Then we analyze the various 802.11 security problems and discuss various ways to improve SOHO wireless security.

Introduction

Wireless local area networks (WLANs) are exploding in popularity, especially in small or home offices (SOHO). While other technologies are available or coming soon, 802.11b devices (also known as Wi-Fi) are now very popular. Just installing a base station and a wireless card in one or more devices (PC, laptop, printer, etc) gives an almost instant mobile network which can use a high-speed internet connection (broadband or dial-up). This is faster, cheaper and much more convenient than running CAT-5 cable and installing outlets, hubs and switches for a traditional Ethernet network which would tie you to a few outlets in your home or office.

In 2001, as 802.11b prices fell and availability and support increased, the popular press began trumpeting this wireless solution. For example, on October 02 David Berlind wrote in *ZD Net*[1] that after studying Wi-Fi for six months, he recommended that no one should deploy wired solutions except to meet special requirements and also recommended Wi-Fi for employees' homes, to move laptops seamlessly between home and office. After acknowledging some well-publicized security problems, Berlind minimized their importance, implying the attacks were too difficult in practice to be much of a threat.

The feedback to his article told a different story. Some were happy with their WLAN; others complained about distance limits; but the first reply was by Scott Jariel[2], who countered Berlind's claims about security one by one and ended with: "start writing about the major lack of security that the technology is creating." Dale Heindel[3] said that his WLAN got very sluggish; when he started to reboot, he got a dialog about how many

---

1 David Berlind, "Look Ma, No Wires!," *ZD Net*, 02 Oct 2001. <http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2815991,00.html>

2 Scott Jariel, "Look Ma, No Wires! -- Talkback," *ZD Net* , 03 Oct 2001 11:44:27. <http://forums.zdnet.com/group/zd.Wireless/it/itupdatetb.tpt/ @thread@1060@forward@1@D-,D@ALL/@article@1060?EXP=ALL&VWM=hr&ROS=1&>

3 Dale Heindel, "Look Ma, No Wires! -- Talkback," *ZD Net* , 05 Oct 2001 09:38:49. <http://forums.zdnet.com/group/zd.Wireless/it/itupdatetb.tpt/ @thread@1075@forward@1@D-,D@ALL/@article@1075?EXP=ALL&VWM=hr&ROS=1>

users were connected to his system. He had to recover Windows ME to get running again. Now he shuts off his wireless access point (AP) when he isn't using it -- this usually keeps his intruder list down to four or less.

One month earlier in *PC Magazine*, Craig Ellison had written about his research showing a majority of 802.11b wireless LANs were vulnerable.[4] Using a laptop with a wireless card and a 14db yagi antenna mounted on a tripod, he quickly identified 61 APs up to six blocks away from the Ziff Davis office in Manhattan. NetStumbler, a shareware program, reported detailed information about each AP, including the fact that the 802.11 Wireless Equivalency Protocol (WEP) was enabled to give privacy on only 21% of the networks. They moved the setup into a vehicle with a GPS unit, drove around for 45 minutes and identified 130 APs (WEP was enabled on 35%).

They repeated this war-driving experiment in the Jersey City financial district (22 APs, with 6 using WEP) and Hoboken (23 APs, with 7 using WEP). They easily found 327 APs in the Boston area, with 31% using WEP. In a trip to Silicon Valley, they found 346 APs, with 152 using WEP. Overall, they found 808 networks with only 38% using WEP security. (Ruth Cowell wrote an very informative paper[5] for GIAC in June of 2001 on war dialing and war driving experiments by Peter Shipley, which also pointed out how insecure most WLANs were.)

Security professionals have reported problems with 802.11 for several years. In October of 1999, Asma Yasmin wrote an early and thorough critique on many 802.11 security issues including weak default configurations leading to interception, theft of services and transitive trust attacks.[6] In Oct 2000, Jesse Walker of Intel wrote that 802.11 security was fundamentally flawed and gave no meaningful privacy at any key size.[7].

In 2001, several new and more powerful threats were reported. Nikita Borisov, Ian Wagner and David Goldberg from UC Berkeley reported[8] how a passive eavesdropper could determine the plaintext from messages using the same initialization vector (IV) and how an attacker could alter and replay a message without detection. Altering the destination of a packet allows an attacker to have the plaintext delivered to himself. They also point out that commercial 802.11b products can be easily used with modified software to perform passive eavesdropping and active insertion attacks.

On Mar 30, William Arbaugh et. al. of the University of Maryland detailed the insecurity of the 802.11 shared key authentication method.[9] Their paper also mentioned that most

---

[4] Craig Ellison, "Exploiting and Protecting 802.11b Wireless Networks," PC Magazine, 04 Sep 2001. <http://www.extremetech.com/print_article/0,3428,a=13880,00.asp>

[5] Ruth Cowell, "War Dialing and War Driving: An Overview," 11 Jun 2001. <http://rr.sans.org/wireless/war.php>

[6] Asma Yasmin, "Known Vulnerabilities in Wirelass LAN Security," 11 Oct 1999. <http://www.tml.hut.fi/Studies/Tik-110.300/1999/Wireless/vulnerability_4.html>

[7] Jesse R. Walker, "Unsafe at any key size; an analysis of WEP encapsulation," 25 Oct 2000. <http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip>

[8] Nikita Borisov, Ian Goldberg and David Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11 (DRAFT)," Jan 2001. <http://www.isaac.cs.berkeley.edu/isaac/wep-draft.html>

[9] William Arbaugh, Narendar Shankar and Y. C. Justin Wan, "Your 802.11 Network has no Clothes," 30 Mar 2001. <http://www.cs.umd.edu/~waa/wireless.pdf>

802.11 cards allow the 48-bit hardware MAC address to be altered by software. This is significant because it puts authorization using access control lists (ACLs) at substantial risk, since MAC addresses are transmitted in the clear for an eavesdropper to pick up. In May, Arbaugh reported a clever chosen plaintext attack[10] that can quickly recover an RC4 encryption stream one byte at a time by trial and error.

The most serious attack was developed by Martin Fluher, Itsik Mantin and Adi Shamir.[11] Based on work in 1995 by Andrew Roos[12] and D. Wagner[13], they discovered how to recover the secret key from the first few bytes of a few thousand messages. In August, Adam Stubblefield, John Ioannidis and Aviel Rubin[14] put together a system with a consumer wireless card and software they wrote in a week -- they used it to recover the 128-bit WEP key for a WLAN. The same month, two products that also implement the Fluher/Mantin/Shamir attack were released with full source code: WEPCrack[15] and AirSnort[16]. All three of these successful attacks work with the widely used PRISM family of WLAN ICs from Intersil[17].

To summarize, most 802.11b networks are used with no security. Even when the maximum security options are selected, standard 802.11b WLANs are completely insecure to a serious attacker. But we still get news like the January 14, 2002, *Computerworld* article[18] that airlines are using insecure WLANs to increase airport security. According to studies reported in this article, all but one administrative WLAN in Denver and all the WLANs operated by American Airlines and Southwest Airlines in San Jose were operating with WEP disabled.

The next four sections of this paper will discuss the 802.11 wireless standards and how they are supposed to provide security. After that, we will examine the weaknesses in detail and see how to get as much security as possible in a typical SOHO environment.

---

[10] William Arbaugh. "An Inductive Chosen Plaintext Attack Against WEP/WEP2," May 2001. <http://www.cs.umd.edu/~waa/attack/frame.htm>

[11] Scott Fluher, Itsik Mantin and Adi Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4," Aug 2001. <http://downloads.securityfocus.com/library/rc4_ksaproc.pdf>

[12] Andrew Roos, "A Class of Weak Keys in the RC4 Stream Cipher," <sci.crypt newsgroup>, 22 Sep 1995. <http://groups.google.com/groups?selm=43u1eh%241j3%40hermes.is.co.za>

[13] D. Wagner, "Re: Weak Keys in RC4," <sci.crypt newsgroup>, 26 Sep 1995. <http://groups.google.com/groups?hl=en&selm=447o1l%24cbj%40cnn.Princeton.EDU>

[14] Adam Stubblefield, John Ioannidis and Aviel D. Rubin, "Using the Fluher, Mantin and Shamir Attack to Break WEP," 06 Aug 2001. <http://www.cs.rice.edu/~astubble/wep/wep_attack.html>

[15] Anton T. Rager, *WEPCrack Project Webpage*, 21 Aug 2001. <http://sourceforge.net/projects/wepcrack/>

[16] Jeremy Brustle and Blake Hegerle, *AirSnort Project Webpage*, 28 Feb 2002. <http://sourceforge.net/projects/airsnort>

[17] Intersil, "PRISM Technology Providers Selection Matrix." <http://www.intersil.com/design/prism/prismuser/index.asp>

[18] Bob Brewin, Dan Verton and Jennifer Disabatino, "Wireless LANs: Trouble n the Air," *Computerworld* 14 Jan 2002. <http://computerworld.com/cwi/story/0,1199,NAV47_STO67344,00.html>

802.11 Basics

The terms 802.11, 802.11b and so on can be confusing. 802.11 is the name of an IEEE standards group, as well as its first WLAN standard. The 802.11 standard contains both a Medium Access Control layer (MAC) specification as well as three physical layer (PHY) specifications that can be used with the MAC. In addition, there are later standards such as 802.11a and 802.11b that define additional PHYs which also use the 802.11 MAC.

The IEEE 802 standards group (http://ieee802.org/) develops LAN/MAN standards, covering Local Area Networks (LANs) and Metropolitan Area Networks (MANs). The IEEE 802.11 Working Group (http://grouper.ieee.org/groups/802/11/main.html) is a subgroup responsible for wireless LAN standards.

IEEE 802 maintains a list of draft and approved standards for subscription.[19] The status of IEEE 802.11 standards and standard activities can be found by searching for 802.11 in the IEEE Standards Status Report.[20] There is also a pilot program that makes single copies of IEEE 802 standards available free for personal use six months after publication.[21]

Here are the current 802.11 standards:

- **802.11-1997** had minor revisions as **802.11-1999**.[22] The 802.11 subgroup has a tutorial on the original 802.11-1997 standard.[23] This describes three (PHYs) and a MAC layer to be used with any of the PHYs:
  - an infrared PHY, which communicates at 1 or 2 Mb/s.
  - a 2.4 GHz radio-frequency PHY using direct sequence spread spectrum modulation (DSSS) to communicate at 1 or 2 Mb/s.
  - a 2.4 GHz radio-frequency PHY using frequency hopping spread spectrum modulation (FHSS) to communicate at 1 Mb/s (and optionally at 2 Mb/s).
  - the MAC layer, which provides data transfer, access control and privacy services.
- **802.11a-1999**[24] defines a 5 GHz PHY that uses orthogonal frequency division multiplexing (OFDM) to communicate at 6, 12 and 24 Mb/s and optionally at 9, 18, 36, 48 and 54 Mb/s, with the first products appearing in 2002. .

---

[19] IEEE, *Local and Metropolitan Area Networks + Drafts (LAN/MAN 802s) Standards Subscription*. <http://standards.ieee.org/catalog/olis/lanman.html>

[20] IEEE, *IEEE Standards Status Report*. <http://standards.ieee.org/db/status/index.shtml>

[21] IEEE, *Get IEEE 802 -- Terms and Conditions*. <http://standards.ieee.org/getieee802/terms.html>

[22] IEEE, "IEEE 802.11-1999 (ISO/IEC 8802-11: 1999), Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications." <http://standards.ieee.org/reading/ieee/std/lanman/802.11-1999.pdf>

[23] Vic Hayes, Greg Ennis, Phil Belanger, Wim Diepstraten, Naftali Chayat and Jan Boer, "Tutorial of draft Standard IEEE 802.11/D3.0," Mar 1996. <http://grouper.ieee.org/groups/802/11/main.htm#Tutorial>

[24] IEEE, "IEEE 802.11a-1999 (ISO/IEC 8802-11:1999/Amd 1:2000(E)), Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Amendment 1: High-speed Physical Layer in the 5 GHz band." <http://standards.ieee.org/reading/ieee/std/lanman/802.11a-1999.pdf>

- **802.11b-1999**[25] (and corrigenda **802.11b-Cor 1-2001**) defines a high rate (HR) DSSS 2.4 GHz PHY communicating at 5.5 and 11 Mb/s in addition to the 1 and 2 Mb/s rates of the 802.11 DSSS PHY. This is done in a compatible way, transmitting headers and control/management frames at one of the lower Basic Service Set (BSS) rates (1 or 2 Mb/s), but switching to higher speeds for data frames. These 802.11b products are very successful, with substantial price drops and explosive growth in product availability in 2001.

Other approved standards include:

- **802.11d-2001** adds requirements and definitions needed to allow 802.11 equipment to operate in more countries.
- **802.1X-2001** for port-based network access control (applies to but not limited to wireless LANs).

Additional standards for WLANs are in progress, including:

- **802.11e** to support for data transport with a specified Quality of Service (QoS).
- **802.11f** to support multi-vendor AP interoperability with an Inter-Access Point Protocol (IAPP).
- **802.11g** for even higher-speed extensions to 802.11b.
- **802.11h** for 5 GHz spectrum and power management extension in Europe.
- **802.11i** to amend 802.11 for improved MAC security.
- **802.1aa** for maintenance and amendments to 802.1X.

802.11 Medium Access Control (MAC)

The 802.11 MAC provides several services that apply to each of the 802.11 PHYs.[26] Data transfer is the MAC's basic service. Data is packaged in chunks called MAC service data units (MSDUs), which are encapsulated and transferred in units called MAC protocol data units (MPDUs) by the lower-level PHY.

The optional privacy service uses the wireless equivalency protocol (WEP) to encrypt data messages. WEP is usually disabled as the default. WEP will be described in detail in the next section.

MAC authentication services are provided to restrict WLAN operation to authorized STAs. 802.11 defines two authentication methods: "Open System" and "Shared Key," although it also allows other methods.

---

[25] IEEE, "IEEE 802.11b-1999 Supplement to 802.11-1999, Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band." <http://standards.ieee.org/reading/ieee/std/lanman/802.11b-1999.pdf>

[26] IEEE, "802.11-1999," pp. 15-33.

The Open System method allows any STA to request authentication, but the AP may deny a request.[27] There are three common AP policies for Open System authentication. First, the AP may allow any station to authenticate -- this is often the default setup. Second, the AP may restrict authentication to stations that transmit a given service set identifier (SSID). This acts somewhat like a password, except that the SSID is also transmitted in the clear by the AP. A third common policy is that some APs restrict access to stations whose MAC address is permitted by the AP's access control list (ACL).

The Shared Key method restricts authentication to STAs which know a secret.[28] Usually, the AP and its intended STAs all share the same key, although the standard allows the AP to use a different key with each STA, based on the STA's MAC address. The Shared Key method requires that the AP and the STAs have WEP privacy enabled, because the STA must successfully encrypt a challenge message in order to be authorized.

To summarize, 802.11 is a family of physical layer protocols. Currently IR and 2.4 GHz and 5 GHz radio media at data rates o1-54 Mb/s are defined. All of these PHYs use the same medium access control layer (MAC) The MAC defines optional privacy (using WEP) and access control (Open System or Shared Key) services in addition to its data transfer service. For ease of installation, the default setup of most 802.11 systems provides little or no security.

Wireless Equivalency Protocol (WEP)

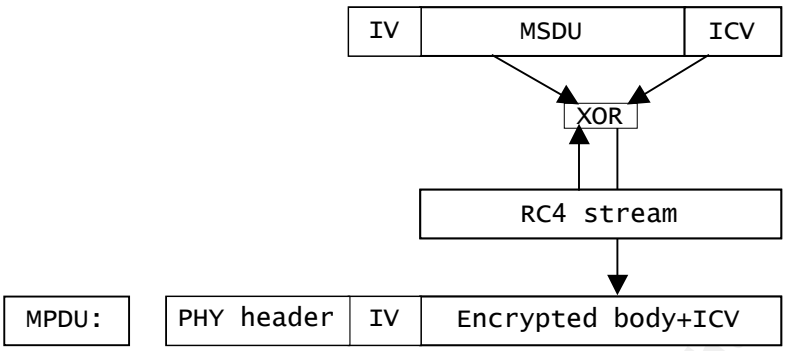
WEP is used to provide privacy for 802.11 data packets.[29] (It is also used in Shared Key authentication.) WEP uses RC4 encryption, a binary additive stream cipher (or Vernam cipher) which is described in more detail in the next section. After initialization by a key, the RC4 algorithm generates a pseudo-random stream which is used to encrypt the plaintext. WEP uses either 64-bit or 128-bit keys. The key consists of either a 40-bit or 104-bit secret value (which all the STAs in a WLAN share) concatenated with a 24-bit initialization vector (IV) chosen by the transmitting STA.

WEP encrypts the frame body (the MSDU in a MPDU) and a 32-bit integrity check value (ICV) by XORing the body and the ICV with a stream of pseudo-random bytes generated by the RC4 encryption algorithm. The RC4 algorithm is reinitialized for each packet with a new IV. Since the AP and the STA share the secret value and the IV is transmitted in the MPDU, the receiver can generate the same RC4 stream and XOR it with the encrypted body to recover the plaintext.

[27] IEEE, "802.11-1999," p. 59.

[28] IEEE, "802.11-1999," pp. 60-61.

[29] IEEE, "802.11-1999," pp. 61-69.



The 802.11 standard specifies that the ICV is to be calculated by a standard CRC, just like the frame check sequence (FCS) which is used in frames that are not encrypted. If the receiver gets a packet that has an invalid ICV or FCS, the packet is silently dropped (except for the encrypted 3rd packet of a Shared Key authorization request.)

The standard recommends but does not require that the IV be changed on every frame. This is to avoid a weakness with this encryption method if the same key is used to initialize the RC4 algorithm for two different packets. Most hardware initializes the IV to zero at power-on and increments it by one after each use.

RC4

RC4 is a stream cipher developed by Ron Rivest at RSA Data Security in 1987. It is proprietary, although the source code was leaked in 1994.[30, 31] Until recently, it has had little cryptographic analysis. Like all stream ciphers, it is unsafe to use the output from a given key to encrypt more than one message.[32]

RC4 is defined as a class of ciphers with different bit lengths, although 8 bits is the size usually used. For this case, RC4 holds an array S of 256 different 8-bit values, plus two indexes into the array (i and j). Initialization uses the key scheduling algorithm (KSA) which sets the array elements to the values 0-255, and then exchanges each element with another element whose position depends on the key. (The key is repeated enough times to provide 256 8-bit values.)

The pseudo-random stream is generated 8-bits at a time by the following procedure. Initially, i and j are set to 0. Then for each output value, i is incremented by 1, j is incremented by S[i], S[i] and S[j] are swapped and then S[S[i]+S[j]] is output.

It is known that there are weak keys which make the first few bytes of the pseudo-random stream less random. In fact, they have a small probability of leaking information about the key.[33]

---

[30] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton: CRC Press, 1997. pp 212, 222.

[31] Roos, "Weak Keys".section 2.

[32] Menezes, *Handbook of Applied Cryptography*, p21.

[33] Fluher, "Weaknesses in RC4."

Perils and Fixes

Between the 802.11 MAC, WEP, RC4 and their implementation in real products, there are many security weaknesses. Some are just terrible design decisions, like not requiring IVs to change. Others are misapplication of otherwise sound components, such as using a stream cipher like RC4 without ensuring unique keys for each message. Some appear to be a failure to consider security implications, such as using a CRC for a message integrity check. Finally, some result from non-security goals, such as supporting open systems. This following sub-sections will identify the known security weaknesses in 802.11 WLANs and what can be done to fix them.

1. Insecure default settings

When **WEP is disabled**, an eavesdropper can monitor all WLAN traffic from many blocks away.[34] This may compromise MAC addresses, Internet addresses, host names, network layout, account names, passwords and personal or sensitive data transmitted over the WLAN. It also allows the network to be used by unauthorized persons, since the SSID and MAC addresses are transmitted in the clear. This may result in loss of bandwidth or attacks on systems in the WLAN or networks connected to it, including denial of service attacks (DoS) against other systems anywhere in the internet.

If **WEP uses 40-bit secret keys**, a brute-force attack on the key is possible.[35] The consequences may be similar to that described above, except that the expectation that WEP privacy is working may result in more sensitive data being transmitted on the WLAN. Note – this is sometimes called 64-bit encryption.

Open Systems authentication allows any station which has a matching SSID to use the WLAN. Many systems have a policy that even allows any station at all to use the WLAN. The Open Systems method is usually the default, since Shared Secret authentication requires WEP, which is often disabled.

Fixes:

Choose to use WEP with 104-bit keys (sometimes called 128-bit encryption.)

Choose an SSID that doesn't give away a lot of information. For example using "XYZ Marketing WLAN" or "1234 Technology Drive" as the SSID gives a lot of information to a potential attacker.

Choose Shared Key authentication.

If the WLAN equipment uses SNMP (and most does), change the default community string and don't use something that is easily guessable . Why lock up your WLAN but leave the tools around to change the lock? Also make sure you secure any other management accesses (such as passwords or other authorization controls for web or telnet access).

---

[34] Ellison, “Exploiting.”

[35] Roos, "Weak Keys," section 2.

2. 802.11 MAC/WEP/RC4 Design Weaknesses

The first weakness is **poor message integrity**, which includes three problems.

- RC4 and the ICV are linear functions, so that it is possible to alter one or more bits in the cipher text and compute the effect this will have on the ICV and the encrypted ICV. This leads to Arbaugh's attack on Shared Key authentication[36], as well as the technique of retransmitting a packet with your own IP address as the destination, so you will receive the unencrypted packet.
- Then the MAC does not require IVs to change. WLAN equipment normally does this, but an attacker can keep on using an IV for which the RC4 stream has been determined. The AP will not recognize an attack might be occurring.
- The MAC also silently discards packets with an incorrect ICV (except for the third packet in an authentication sequence).. Due to the noisy nature of WLANs, this avoids a lot of spurious reports, but it can hide attacks. This allows Arbaugh's chosen-plaintext attack to succeed.[37]

The second design weakness is allowing **repeating keys for a stream cipher.** The WEP design of using only 24-bit IVs and allowing them to start at zero at power-on means that all the STAs in a WLAN using WEP will probably use the same IVs as the AP did when it started operating. Furthermore, on a busy WLAN, IVs have to repeat several times a day. This was a terrible set of design decisions, because any stream cipher, such as RC4 allows easy attacks if the same key is used on two different messages.[38]

The third design weakness is **lack of secure two-way authentication.**[39] The 802.11 MAC provides a Shared Key authentication method that can be compromised. If any successful Shared Key authentication is monitored, an intruder can use the message integrity weaknsses to construct a valid answer to any other challenge.

In addition, since the AP does not authenticate itself, an attacker can pretend to be an AP to a STA and then turn around and act as the STA to a real AP (this a man-in-the-middle attack).[40]

The fourth design weakness is using **unauthenticated management messages**. This allows an attacker to send a Disassociate or Deauthorize message to an authenticated STA and then take its place. This is called session hijacking.[41]

The fifth weakness is using **RC4 with unscrambled keys.** The RC4 algorithm has a weak KSA that has a slight probability of leaking information about the key for the

---

[36] Arbaugh, “Network has no Clothes.”

[37] Arbaugh, "Chosen Plaintext".

[38] Roos, "Weak Keys," section 2.

[39] Arunesh Mishra and William A. Arbaugh, "An Initial Security Analysis of the IEEE 802.1X Standard," 06 Feb 2002. <http://www.cs.umd.edu/Library/TRs/CS-TR-4328/CS-TR-4328.ps.Z> section 4.1.

[40] Arunesh, "Security of 802.1X," section 4.2.

[41] Arunesh, "Security of 802.1X," section 4.1.

first few bytes of the pseudo-random stream. According to Ron Rivest, the inventor of RC4, hashing the key or discarding the first few hundred bytes of the pseudo-random stream makes it much more resistant to attack.[42]

Fixes:

Fixes for these problems are harder. **802-11i** has some proposed changes out for ballot at this time. I believe they include using a unique RC4 master key for each pair of stations, derived by scrambling the secret value with the AP and STA addresses and using odd IVs for one direction and even IVs for the reverse direction. They also update the master key before repeating any IVs. I hope 802.11i will fix the other design problems as well.

Unfortunately, we have the double hurdle of waiting for approval of the revised standard and then waiting for products to support it or upgrades for products already sold. Interoperability with existing equipment will probably be interesting, as well. So, maybe we wait.

An alternative is to use a single-vendor solution that gives additional security like **RADIUS authentication**, such as the Cisco Aeronet 350.[43] Disadvantages are cost and lack of interoperability as the tradeoff for more security.

You might also consider alternatives to 802.11b. **802.11a** will be subject to the same design weaknesses and eventual fixes, but considerably faster. **Bluetooth** has better security, but it is slower and still has some security issues. **HomeRF** promises that nobody will be able to eavesdrop because it uses frequency hopping, with a schedule that depends on the key.[44]

Another area to consider is defense in depth. You probably should install a **firewall** [45] to protect the rest of your network from the WLAN (assume it is wide open -- it just might be.)

A Virtual Private Network (**VPN**) can be effective if you have a VPN server for your needs.[46] A VPN to a work network is very feasible, but doesn't protect you when you are connecting to other network sites. Perhaps there is a maket for an AP with a build-in VPN server.

---

[42] Ron Rivest, "RSA Security Response to Weaknesses in Key Scheduling Algorithm of RC4," 01 Sep 2001. <http://www.rsasecurity.com/rsalabs/technotes/wep.html>

[43] Robert Sprague, "Cisco's Aironet 350 – An Enterprise-Level Wireless Security Solution," 28 Sep 2001. <http://rr.sans.org/wireless/aironet350.php>

[44] Bob Szacik, "HomeRF: Wireless with Security, for the Rest of Us?," 18 May 2001. <http://rr.sans.org/wireless/homerf.php>

[45] SANS Institute, *Firewall and Perimeter Protection Webpage*, 06 Mar 2002. <http://rr.sans.org/firewall/firewall_list.php>

[46] SANS Institute, *Encryption and VPNs Webpage*, 28 Feb 2002. <http://rr.sans.org/encryption/encryption_list.php>

Summary

802.11b WLANs are very popular, but there are huge security problems with present implementations. 802.11a is going to become very popular in 2002, but it will have the same problems until the 802.11i changes are approved and implemented. In the meantime, enable all the security you can (maybe the bad guys will attack someone easier), use defense in depth and worry a lot until the known security problems are fixed.

References

1. Arbaugh. William. "An Inductive Chosen Plaintext Attack Against WEP/WEP2." May 2001. <http://www.cs.umd.edu/~waa/attack/frame.htm>
2. Arbaugh, William; Narendar Shankar and Y. C. Justin Wan. "Your 802.11 Network has no Clothes." 30 Mar 2001. <http://www.cs.umd.edu/~waa/wireless.pdf>
3. Mishra, Arunesh and William A. Arbaugh. "An Initial Security Analysis of the IEEE 802.1X Standard." 06 Feb 2002. <http://www.cs.umd.edu/Library/TRs/CS-TR-4328/CS-TR-4328.ps.Z>
4. Berlind, David. "Look Ma, No Wires!" *ZD Net*, 02 Oct 2001. <http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2815991,00.html>
5. Borisov, Nikita; Ian Goldberg and David Wagner. "Intercepting Mobile Communications: The Insecurity of 802.11 (DRAFT)." Jan 2001. <http://www.isaac.cs.berkeley.edu/isaac/wep-draft.html>
6. Brewin, Bob; Dan Verton and Jennifer Disabatino. "Wireless LANs: Trouble n the Air." *Computerworld*. 14 Jan 2002. <http://computerworld.com/cwi/story/0,1199,NAV47_STO67344,00.html>
7. Brustle, Jeremy and Blake Hegerle. *AirSnort Project Webpage*. 28 Feb 2002. <http://sourceforge.net/projects/airsnort>
8. Cisco Systems, Inc. "Cisco Aironet 350 Series Wireless LAN Security." 01 Nov 2001. <http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm>
9. Cowell, Ruth. "War Dialing and War Driving: An Overview." 11 Jun 2001. <http://rr.sans.org/wireless/war.php>
10. Delio, Michelle. "Wireless Networks in Big Trouble." *Wired News*. 02 Aug 2001. <http://www.wired.com/news/wireless/0,1382,46187,00.html>
11. Ellison, Craig. "Exploiting and Protecting 802.11b Wireless Networks" PC Magazine. 04 Sep 2001. <http://www.extremetech.com/print_article/0,3428,a=13880,00.asp>
12. Evans, William F. "RADIUS – A Protocol for Centralized Authentication." 27 Oct 2000. <http://rr.sans.org/authentic/radius2.htm>
13. Fluher, Scott; Itsik Mantin and Adi Shamir. "Weaknesses in the Key Scheduling Algorithm of RC4." Aug 2001. <http://downloads.securityfocus.com/library/rc4_ksaproc.pdf>

14. Hayes, Vic; Greg Ennis; Phil Belanger; Wim Diepstraten; Naftali Chayat and Jan Boer. "Tutorial of draft Standard IEEE 802.11/D3.0." Mar 1996. <http://grouper.ieee.org/groups/802/11/main.htm#Tutorial>

15. Heindel, Dale. "Look Ma, No Wires! -- Talkback." *ZD Net*. 05 Oct 2001 09:38:49. <http://forums.zdnet.com/group/zd.Wireless/it/itupdatetb.tpt/@thread@1075@forward@1@D-,D@ALL/@article@1075?EXP=ALL&VWM=hr&ROS=1>

16. IBM Corporation. "Wireless Security Auditor (WSA)." <http://www.research.ibm.com/gsal/wsa>

17. IEEE. *Get IEEE 802 -- Terms and Conditions*. <http://standards.ieee.org/getieee802/terms.html>

18. IEEE. "IEEE 802.11-1999 (ISO/IEC 8802-11: 1999), Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications." <http://standards.ieee.org/reading/ieee/std/lanman/802.11-1999.pdf>

19. IEEE. "IEEE 802.11a-1999 (ISO/IEC 8802-11:1999/Amd 1:2000(E)), Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Amendment 1: High-speed Physical Layer in the 5 GHz band." <http://standards.ieee.org/reading/ieee/std/lanman/802.11a-1999.pdf>

20. IEEE. "IEEE 802.11b-1999 Supplement to 802.11-1999, Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band." <http://standards.ieee.org/reading/ieee/std/lanman/802.11b-1999.pdf>

21. IEEE. *IEEE Standards Status Report*. <http://standards.ieee.org/db/status/index.shtml>

22. IEEE. *Local and Metropolitan Area Networks + Drafts (LAN/MAN 802s) Standards Subscription*. <http://standards.ieee.org/catalog/olis/lanman.html>

23. Internet Security Systems. "Wireless LAN Security: 802.11b and Corporate Networks." <http://documents.iss.net/whitepapers/wireless_LAN_security.pdf>

24. Intersil. "PRISM Technology Providers Selection Matrix." <http://www.intersil.com/design/prism/prismuser/index.asp>

25. Jariel, Scott. "Look Ma, No Wires! -- Talkback" *ZD Net*. 03 Oct 2001 11:44:27. <http://forums.zdnet.com/group/zd.Wireless/it/itupdatetb.tpt/@thread@1060@forward@1@D-,D@ALL/@article@1060?EXP=ALL&VWM=hr&ROS=1&>

26. Kabara, Joseph; Prashant Krishnamurthy and David Tipper. "Information Assurance in Wireless Networks." Sep 4, 2001. <http://www.cert.org/research/isw/isw2001/papers/Kabara-31-08.pdf>

27. Mehta, Princy C. "Wired Equivalency Privacy Vulnerability". 04 Apr 2001. <http://rr.sans.org/wireless/equiv.php>

28. Menezes, Alfred J.; Paul C. van Oorschot and Scott A. Vanstone. *Handbook of Applied Cryptography*. Boca Raton: CRC Press, 1997.

29. Mobile Computing Online. "Comparison Report: Wireless LANs for All: Aironet 350". <http://www.mobilecomputing.com/showarchives.cgi?149:4>

30. Molta, Dave. “Cisco Aironet 350 Series Tightens Wireless Security.” 05 Feb 2001. <http://www.networkcomputing.com/1203/1203sp1.html>

31. Nelson, Matthew G. "Untethered Doesn’t Mean Unsecure." 05 Feb 2001. <http://www.informationweek.com/shared/printArticle?article=infoweek/823/cisco.htm&pub=iwk >

32. Publications and Communications, Inc. "Cisco and Microsoft Collaborate on Wireless Networking Security." *Cisco World*. May 2001. <http://www.ciscoworldmagazine.com/monthly/2001/05/microsoft.shtml>

33. Rager, Anton T. *WEPCrack Project Webpage*. 21 Aug 2001. <http://sourceforge.net/projects/wepcrack/>

34. Rivest, Ron. "RSA Security Response to Weaknesses in Key Scheduling Algorithm of RC4." 01 Sep 2001. <http://www.rsasecurity.com/rsalabs/technotes/wep.html>

35. Roos, Andrew. "A Class of Weak Keys in the RC4 Stream Cipher." <sci.crypt newsgroup>. 22 Sep 1995. <http://groups.google.com/groups?selm=43u1eh%241j3%40hermes.is.co.za>

36. Ross, B. Justin. “Containing the Wireless LAN Security Risk.” 04 Nov 2000. <http://rr.sans.org/wireless/wireless_LAN.php>

37. SANS Institute. *Encryption and VPNs Webpage*. 28 Feb 2002. <http://rr.sans.org/encryption/encryption_list.php>

38. SANS Institute. *Firewall and Perimeter Protection Webpage*, 06 Mar 2002. <http://rr.sans.org/firewall/firewall_list.php>

39. Schenk, Rob. "Cisco Aironet 350 Series." 15 Feb 2001. <http://www.zdnet.com/products/stories/reviews/0,4161,2682131,00.html>

40. Sprague, Robert. “Cisco’s Aironet 350 – An Enterprise-Level Wireless Security Solution.” 28 Sep 2001. <http://rr.sans.org/wireless/aironet350.htm>

41. Stubblefield, Adam; John Ioannidis and Aviel D. Rubin. "Using the Fluher, Mantin and Shamir Attack to Break WEP." 06 Aug 2001. <http://www.cs.rice.edu/~astubble/wep/wep_attack.html>

42. Szacik, Bob. "HomeRF: Wireless with Security, for the Rest of Us?" 18 May 2001. <http://rr.sans.org/wireless/homerf.php>

43. Wagner, D. "Re: Weak Keys in RC4." <sci.crypt newsgroup>. 26 Sep 1995. <http://groups.google.com/groups?hl=en&selm=447o1l%24cbj%40cnn.Princeton.EDU>

44. Walker, Jesse R. "Unsafe at any key size; an analysis of WEP encapsulation." 25 Oct 2000. <http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip>

45. Wang, Sean. "Threats and Countermeasures in Wireless Networking." 20 Dec 2000. <http://rr.sans.org/wireless/threats.php>

46. Yasmin, Asma. "Known Vulnerabilities in Wirelass LAN Security." 11 Oct 1999. <http://www.tml.hut.fi/Studies/Tik-110.300/1999/Wireless/vulnerability_4.html>

Last Updated: June 26th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SEC564:Red Team Ops	OnlineCAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced