

Wireless Insecurity / How Johnny can hack your WEP protected 802.11b Network!

Soumendra Nanda, Dartmouth College
snanda@cs.dartmouth.edu

Summary:

This paper is an up to date look at various problems inherent in today's wireless networks from a user as well as administrator's point of view. The wireless medium makes eavesdropping a major threat, interference a problem, and the interception of transmissions easier than on wired networks. Several security problems and threats are exposed in detail along with descriptions on how to exploit them. The paper concludes with a look at guidelines to ensuring the security of these networks and preventing the attacks described in this paper.

The outline is as follows:

Section 1 gives an introduction to wireless networks and the standards involved. Section 2 explains the theory and procedures behind the recently discovered attacks specifically on 802.11 networks in detail. Section 3 concludes with a set of guidelines for securing wireless LANs and a look at some proposed solutions.

1 Introduction:

In today's fast changing world management of information is the key to corporate success. This goes hand-in-hand with communication infrastructure. Of late there have been a tremendous growth in wireless LAN usage, a growth that is compared by many to be almost as the phenomenal as that of the Internet in the 90s.

The key factors driving this growth have been decreasing costs, increasing speeds and the general convenience of not having to run wires and not being limited to fixed network access points. While wireless LANs are not likely to replace all wired LANs any time soon (if ever), the two are already beginning to coexist almost seamlessly in several academic, corporate and home environments. Current wireless technology allows throughputs as high as 11 Mbps and efforts are on to go beyond this limit. Another key factor in the growth of wireless LAN usage has been the move by vendors towards standardization of protocols and equipment.

Access to a wired LAN is governed by access to an Ethernet port for that LAN. Therefore, access control for a wired LAN often is viewed in terms of physical access to LAN ports. Similarly, because data transmitted on a wired LAN is directed to a particular destination, privacy cannot be compromised unless someone uses specialized equipment to intercept transmissions on their way to their destination. In short, a security breach on a wired LAN is possible only if the LAN is physically compromised.

With a wireless LAN (WLAN), transmitted data is broadcast over the air using radio waves. Thus it can be received by any WLAN client in the area served by the data transmitter. Because radio waves travel through ceilings, floors, and walls, transmitted data may reach unintended recipients on different floors and even outside the building of the transmitter. Installing a WLAN may seem like putting Ethernet ports everywhere including your parking lot! Similarly, data privacy is a genuine concern with wireless LANs because there is no way to direct a WLAN transmission to only one recipient.

1.1 IEEE standard LANs

In 1999, the Institute of Electrical and Electronics Engineers (IEEE) ratified an extension to a previous standard called the IEEE 802.11b [1]. It defines the standard for wireless LAN products that operate at an Ethernet-like data rate of 11 Mbps, a speed that makes wireless LAN technology viable in enterprises and other large organizations. Interoperability of wireless LAN products from different vendors is ensured by an independent organization called the Wireless Ethernet Compatibility Alliance (WECA) which brands compliant products as "Wi-Fi"[2]. Dozens of vendors market Wi-Fi products and organizations of every size and type are considering, if not deploying, such wireless LANs. The last official update to the protocol was in June 2001[3].

IEEE 802.11b devices use the 2.4GHz frequency range. Using this range in certain environments can cause certain problems. 802.11b doesn't work well around operating microwave ovens, 2.4GHz cordless telephones, and Bluetooth devices. However efforts are on to solve the problem of interference between Bluetooth and Wi-Fi. [4]

WEP

The IEEE 802.11b standard stipulates an optional encryption scheme called Wired Equivalent Privacy, or WEP that offers a mechanism for securing wireless LAN data streams. WEP uses a symmetric scheme in which the same key and algorithm are used for both encryption and decryption of data. The goals of WEP included:

Access control: To prevent unauthorized users who lack a correct WEP key from gaining access to the network.

Privacy: To protect wireless LAN data streams by encrypting them and allowing decryption only by users with the correct WEP keys.

Although WEP is optional, support for WEP with 40-bit encryption keys is a requirement for Wi-Fi certification by WECA, so WECA members invariably support WEP. We will see more details about WEP and its weaknesses in the rest of this paper. An IEEE task force is working to come up WEP2 to solve problems and weaknesses known in the current implementation.

1.2 Bluetooth, the Viking

Bluetooth, named after the Viking, Harald Bluetooth, is a standard developed by IBM [5] which has slightly different application intended for it. It was designed for use in small portable devices such as hands-free phone headsets, stereo headphones, laptops, PDA devices and other electronic appliances. The first device revealed for the standard was a hands-free headset by Ericsson for a cell phone that networks with a wireless attachment to a cell phone.

Some of the security measures include a 48 bit public address that is unique for each user, two secret keys, and a random number, different for each new transaction. The secret keys are generated during initialization and are never disclosed. Normally, the encryption key is derived from the authentication key during the authentication process. For the authentication algorithm, the size of the key used is always 128 bits. For the encryption algorithm, the key size might vary between 1 and 16 octets (8 - 128 bits). The key size is user-configurable, which has the advantage of allowing the user to be as paranoid as he wants to be.

1.3 Other Standards

Some of the other wireless standards not described here but may be prevalent some day are 802.11a, HiperLan-2 and 5-Unified Protocol (5-UP). [5]

2. Here Lie Dragons

2.1 War Driving

Of late there have been several articles in the press regarding weaknesses in 802.11 WLANs. Some of the most notable stories have been about “war driving” [6] [7]. War driving is a term coined recently to refer to security experts and hackers alike who simply drive by metropolitan areas (sometimes as fast as 55 miles per hour!) and expose wireless LANs. They do this as they go along by scanning, analysis and triangulation. In over 60% of the cases the security has proven to be absolutely none! The tools used are alarmingly inexpensive and easy to obtain. Basically all that is needed is a laptop, a wireless PCMCIA card and an antenna. The software for these attacks is easily available off the web and is open source. These efforts have exposed over a thousand WLANs open to intruders in Manhattan, the Bay Area and New England.

Shipley goes on to show how he manages to attack Wireless LANs remotely from as far as 25 miles away [7] using more powerful equipment like YAGI antennas. Such equipment is not prohibitively expensive either as can be seen from this article showing how to make one at home [8]. The ability to attack a LAN from such a distance raises some serious legal issues, one of the most poignant being what if the attacker was in a foreign embassy on foreign soil in a city like Washington, DC.

The publicity about wireless LAN security, oddly enough, has not yet included exploits by the hacker community. So far war driving has been used largely to find networks, not to penetrate them. In the near future, however, expect to hear that wireless networks have been hacked, viruses have proliferated through such networks, and expect much greater havoc than has been reported yet. [9]

2.2 WEP's Detailed Flaws

So how did they actually do this? In order to understand the issues involved we have to take a closer look at WEP and the internal workings of 802.11 networks.

Authentication

A client cannot participate in a wireless LAN until that client is authenticated. The IEEE 802.11b standard defines two types of authentication methods: open and shared key. The authentication method must be set on each client, and the setting should match that of the access point with which the client wants to associate.

With open authentication, which is the default, the entire authentication process is done in clear-text, and a client can associate with an access point even without supplying the correct WEP key. With shared-key authentication, the access point sends the client a challenge text packet that the client must encrypt with the correct WEP key and return to the access point.

Service Set Identifier SSID

One commonly used wireless LAN feature is a naming handle called an SSID, which provides a rudimentary level of access control. An SSID is a common network name for the devices in a wireless LAN subsystem; it serves to logically segment that subsystem. The use of the SSID as a handle to permit/deny access is dangerous because the SSID typically is not well secured. [10] An access point, the device that links wireless clients to the wired LAN, usually is set to broadcast its SSID in its beacons. SSIDs can also

be guessed easily in general and are very often unassigned or set to manufacturers default values. In the worst case you could resort to one of the 3 Bs, Burglary, Bribery or Blackmail to get an SSID for a target LAN. All users must use the same SSID to access their network.

WEP 1.0

WEP uses the RC4 stream cipher that was invented by Ron Rivest of RSA Data Security Inc for encryption. The RC4 encryption algorithm is a symmetric stream cipher that supports a variable length key. The IEEE 802.11 standard describes the use of the RC4 algorithm and the key in WEP. However, key distribution or key negotiation is not mentioned in the standard and is left to the vendor to implement.

The WEP protocol upon which 802.11b WLANs depend for encryption, authentication and repudiation of data is riddled with fundamental architectural flaws. The initialization vector (IV) that's generated every time a Wi-Fi Network Interface Card (NIC) powers up is a maximum of just 24 bits long -- and some cards simply give it an initial value of 0 and then increment that value by 1 every time they send or receive a packet.

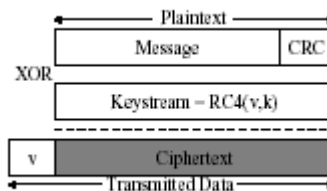


Figure 1 Encrypted WEP frame

Basic Encryption Mechanism

The RC4 algorithm generates a keystream (a long sequence of pseudorandom bytes) as a function of the IV and the secret key k . This keystream is denoted by $RC4(v, k)$. Then we exclusive-or (XOR) the plaintext with the key stream to obtain the ciphertext C from plaintext P :

$$C = P \oplus RC4(v, k)$$

Decryption:

It is a simple reverse operation at the recipient's end.

$$\begin{aligned} P' &= C \oplus RC4(v, k) \\ &= (P \oplus RC4(v, k)) \oplus RC4(v, k) \\ &= P \end{aligned}$$

2.3 The Attacks Explained

One of the simplest attacks described in [11] is to find two packets with the same IV and secret key and XOR them together. The result is the XOR of the two original plaintexts. If one of the plaintexts is known, it is trivial to find the other one. Several other simple passive attacks are mentioned in that paper to analyze and decrypt stored packets and a few active ones involving injecting false packets into the network.

Decryption of captured packets became much easier after this paper [12] was released often referred to as the FMS attack. The Fluhrer, Mantin, and Shamir known IV attack utilizes the fact that, in some cases, knowledge of the IV and the first output byte leaks information about the key bytes. They refer to these

key-leaking cases as resolved cases. By looking at a number of these resolved cases, we can see a bias toward the true key bytes. The group that discovered this attack had not verified it experimentally. This attack was first implemented in August 2001 by Stubblefield et al [13] however they did not make their source available publicly.

Two software projects that have implemented the same attack and are available as open source are AirSnort [14] and WEPCrack [15]. Air Snort integrates a packet sniffer with a decryption attack working in parallel. It needs to collect generally between 100,000 to 1 Million packets (about 100Mb to 1Gb) and then can return a 128 bit encryption key in seconds. WEPCrack analyzes packets collected by a popular open source packet sniffer called ethereal. Both work under Linux with wireless cards that use the PRISM 2 chipset, which is one of the most common ones available and can easily be configured to run in promiscuous mode.

The bottom line is using these tools it would take at most a day to crack any WEP enabled wireless LAN that an attacker can monitor. The tools used by the war drivers were similar. In addition they used GSM software to triangulate and pinpoint geographically various access points they had discovered. They simply sniffed out wireless LANs that allow roaming access and have their SSIDs set to "ANY"/ broadcast mode. Thus armed with these newer tools hackers potentially have much more firepower. In retrospect if the WEP draft had been made public for peer review before it was implemented this situation could certainly have been avoided.

2.4 WEP2 A Flawed Proposal!

The IEEE standards board is rather aware of all these recent attacks and exposed vulnerabilities. They drafted a standard known as WEP2 to solve the current batch of problems. One of their recommendations is that the IV be increased to 128 bits from the current value of 24. There is also a provision for mandatory Kerberos version V authentication which brings with it exposure to dictionary attacks amongst many others! [16] The new version proposed is still vulnerable to replay attacks and is very vulnerable to denial of service attacks as seen in Aboba's analysis [17]. The only problem it appears to have solved is that it prevents being hacked by the current set of war driving and WEP cracking tools. Aboba recommended looking at other solutions like SRP or EAP-SRP.

In fact, at the May 14-18, 2001 meeting of the IEEE's 802.11 full working group at the Universal City Radisson Hotel in Orlando, FL, a motion to remove WEP2 from the next draft of the 802.11 spec failed by a very close vote of 30 to 36 with one abstention [18].

3 Real World Solutions

3.1 A Quick Fix from RSA

When the attacks were first exposed by FMS and Stubblefield et al, RSA Labs was the first to respond claiming it had a simple solution to the problem called "Fast Packet Keying" [19] that basically changes how IVs are generated and fixes the weakness in RC4. The IEEE 802.11 committee has accepted the "Fast Packet Keying" technology and agreed to adopt it soon, but it's not clear when wireless LAN vendors will make Fast Packet Keying available as either a software or firmware patch. However solutions like these may make interoperability of equipment a problem and customers may be limited to purchasing from only certain vendors.

3.2 802.1X

The task of defining the interaction between IEEE 802.1X and 802.11 has been given to IEEE 802.11 Task Group I (Security), which is in the process of completing its recommendations. IEEE 802.1X provides an authentication framework for wireless LANs, allowing a user to be authenticated by a central authority. The actual algorithm that is used to determine whether a user is authentic is left open and multiple algorithms are possible. 802.1X uses an existing protocol, the Extensible Authentication Protocol (EAP, RFC 2284) that works on Ethernet, token ring, or wireless LANs, for message exchange during the authentication process.

802.1X Basics

In a wireless LAN with 802.1X, a user (known as the supplicant) requests access to an access point (known as the authenticator). The access point forces the user (actually, the user's client software) into an unauthorized state that allows the client to send only an EAP start message. The access point returns an EAP message requesting the user's identity. The client returns the identity, which is then forwarded by the access point to the authentication server, which uses an algorithm to authenticate the user and then returns an accept or reject message back to the access point. Assuming an accept was received, the access point changes the client's state to authorized and normal traffic can now take place. The authentication server may use the Remote Authentication Dial-In User Service (RADIUS), although 802.1X does not specify it.

Authentication Weakness

In a recently paper published [20], the authors Arbaugh and Mishra, expose the fact that the 802.1X protocol is severely flawed for a very simple reason, the authentication protocol is only one sided i.e. there is no mutual authentication. The problem found by the authors is that while 802.1X lets the network access point make sure the user is authentic, it fails to provide a reciprocal method by which the user can guarantee the authenticity of the access point. This exposes the system to “Man in the Middle Attacks” and session hijacking. The paper also describes ways to carry out Denial of Service attacks.

802.1X: A Work in Progress

In their paper [20], the authors state that the draft standard for 802.1x does not support mutual authentication by default. 802.1x is still a draft proposal and yet to be finally approved in its current state. There is a specification in it to use the EAP-TLS protocol, which does provide mutual authentication. Thus some of the flaws pointed out by the authors in [20] are highly implementation dependent.

In fact Aboba et al proposed mutual authentication for 802.1x as early as May 2000 [21]. Cisco has already introduced products based on the 802.1x protocol and they claim to have implemented mutual authentication protocols as default in their products [22]. However they do admit that their product is vulnerable at present to packets being tampered undetected due to how the CRC (Circular Redundancy Check) Checksums are calculated.

CRC-32 Checksum Issues

The integrity check function of the 802.11 standard is vulnerable because it uses a linear CRC-32 checksum, making it possible to compute the differences between two CRCs by flipping bits in a message. Neither the 802.1x nor the existing 802.11 standard address this issue. One proposed solution is to use a per packet message integrity check in the future.

3.3 No Single Security Solution Fits All

Securing the WLAN is just one component of the overall enterprise security framework. Security experts recommend that enterprises deploy several layers of defense across the network to mitigate threats. Additional security components might include firewalls, intrusion detection systems, and segmenting networks.

A lot of solutions involve use of RADIUS for authentication mechanisms. Though not an official standard, the RADIUS specification is maintained by a working group of the Internet Engineering Task Force (IETF). Here again caution is advisable due to several implementation dependent flaws discovered as recently as March 4^h, 2002 [23] which make the system susceptible to Denial of Service attacks and other flaws which are related to the limited key space available for setting system passwords.

3.4 Practical Advice:

For a start if you use a wireless 802.11x device enable WEP. Most users simply leave it turned off by default. Yes it can be cracked but at least you don't hand everything over to your attacker/ adversary on a platter. Make sure you change the manufacturers default keys and set your own. Any attacker worth his salt knows all the default keys. Updating your firmware and software as often as possible is a no-brainer but here can prove to be vital to the networks survival.

Disable use of "broadcast mode" at the access points (AP). This forces only devices with valid SSIDs to associate with that AP. Selecting a good SSID is also important. A good SSID should be complicated d should not be easily guessed.

If you have a very small WLAN then consider turning DHCP off and assigning static IPs. This would help make the attackers job a little more complicated.

Monitor the MAC addresses of the devices trying to associate with an AP. This may lead to huge tables but should definitely help in intrusion detection, simply because forging MAC addresses is much harder than forging IP addresses. [24] There has also been some research in tools used to detect packet sniffers and several tools used in wired LANs could probably be used here as well.

Some security experts suggest looking at how the Japanese have been successful with the DoCoMo phone system with about a thousand participating merchants and using SSL for secure transactions. They suggest an application-layer encryption method (SSL, SSH) for all communication, or better still, a TCP/IP layer encryption like IPsec. [25]

3.5 DMZ and VPN

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 (De Militarized Zone) [26], and have your wireless users tunnel into your network using a Virtual Private Network .If your corporation doesn't already have a VPN infrastructure in place, it's going to cost 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.

Finally get a third party to audit your network or better still get a laptop load it with a wireless card, Linux and the latest auditing software and see how much exposed it really is! There are several solutions available corporate as well as academic and one of them is IBM's Wireless Security Auditor (WSA) [27] project aimed at network administrators and laymen who only have basic knowledge using a Compaq Ipaq PDA running Linux and some additional devices and tools.

It is expected that the IEEE will finalize its new standards by the end of 2002[28].

4 Conclusions

The conclusion is quite simple, wireless networks using the 802.11b protocol are at present inherently insecure and vulnerable to a variety of attacks. Using a laptop with a Wi-Fi card and the right software, an attacker is capable of immense mischief and in theory could be as far as 20 miles away in a safe haven. Networks which are poorly configured or do not have any encryption being utilized are the most vulnerable. Recent efforts have shown the potential weakness in the draft specifications for 802.1x protocol and it is hoped that the IEEE can now correct these before rolling out the final standards and specifications since they can be used to provide added security to WLANs. Several alternate solutions are still possible for securing a wireless network but most of them require careful design, planning and engineering.

References:

[1] IEEE 802.11 Working Group for Wireless LANs
<http://www.ieee802.org/11/>

[2] WECA Wireless Ethernet Compatibility Alliance
<http://www.wirelessetehrnet.com>

[3] IEEE 802 Standards Download Page
<http://standards.ieee.org/catalog/olis/lanman.html>

[4] What's what in Wireless today
By L Victor Marks, IBM Corporation, May 2001
<http://www-106.ibm.com/developerworks/library/wi-what/>

[5] Coexistence of 802.11b and Bluetooth
http://www.mobilian.com/documents/Coexistence_of_802.11b_and_Bluetooth1.pdf
*

[6] Exploiting and Protecting 802.11b Wireless Networks
By: Craig Ellison, PC Magazine September 4, 2001
http://www.extremetech.com/print_article/0,3428,a=13880,00.asp

[7] Mike Shipley's Presentation on War Driving: Open WLANS
<http://www.dis.org/filez/openlans.pdf>

[8] How to build a YAGI antenna from a "Pringles Can"
<http://www.oreillynet.com/cs/weblog/view/wlg/448>

[9] The Limits on Wireless Security: 802.11 in early 2002 by James Voorhees January 30, 2002
<http://rr.sans.org/wireless/limits.php>

- [10] Security for Next Generation Wireless LANs. Cisco Corporation White Paper, 2001
<http://www.cisco.com/warp/public/102/wlan/nextgen.pdf>
- [11] Intercepting Mobile Communications: The Insecurity of 802.11 by Nikita Borisov, Ian Goldberg, David Wagner, UC Berkeley 2001
- [12] Weaknesses in the key scheduling algorithm of RC4 by Fluhrer, Mantin, and Shamir, August 2001.
- [13] Using the Fluhrer, Mantin, and Shamir Attack to Break WEP by Stubblefield, Ioannidis and Rubin, August 2001
- [14] AirSnort Project Homepage
<http://airsnort.sourceforge.net>
- [15] WEPCrack Project Homepage
www.wepcrack.sourceforge.net
- [16] A Real-World Analysis of Kerberos Password Security by Thomas Wu, Stanford University 1998
<http://theory.stanford.edu/~tjw/krbpass.html>
- [17] Presentation on WEP2 Bernard Aboba, Microsoft May 2001
<http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/1-253.zip>
- [18] WEP2 Credibility Zero, by Jonathan Stark, April 2001
<http://www.starkrealities.com/wireless003.html>
- [19] RSA Labs Fast Keying fix for WEP
<http://www.rsasecurity.com/rsalabs/technotes/wep-fix.html>
- [20] An Initial Security Analysis Of 802.1x by William Arbaugh and Anuresh Mishra, University of Maryland Feb 20 2002
<http://www.cs.umd.edu/~waa/1x.pdf>
- [21] Security issues in 802.1x D Simon, Bernard Aboba, and Tim Moore of Microsoft Corporation March 2000 <http://www.ieee802.org/1/mirror/8021/docs2000/8021xSecurity.PDF>
- [22] Securing the Wireless LAN: BY Gail Meredith, Cisco Corporation July 2001
<http://www.cisco.com/warp/public/784/packet/jul01/p74-cover.html>
- [23] CERT advisory on RADIUS vulnerabilities, March 4 2002
<http://www.cert.org/advisories/CA-2002-06.html>
- [24] Exploiting and Protecting 802.11b Wireless Networks by Craig Ellison, PC Magazine, Sept 4 2001
http://www.extremetech.com/print_article/0,3428,a=13880,00.asp
- [25] Using IPSec to Construct Secure Virtual Private Networks: IBM White Papers
<http://www-3.ibm.com/software/network/library/whitepapers/vpn/>
- [26] Designing a DMZ by Scott Young, March 26, 2001
<http://rr.sans.org/firewall/DMZ.php>
- [27] WSA Project home, IBM Corporation
www.research.ibm.com/gsal/wsa/
- [28] The Unofficial 802.11 Security Page maintained by Bernard Aboba
<http://www.drizzle.com/~aboba/IEEE/>