SECURITY ISSUES OF THE IEEE 802.11B WIRELESS LAN

Hamid Boland and Hamed Mousavi
Carleton University
hboland@ieee.org and hamed@ieee.org

Abstract

The IEEE 802.11 wireless LAN standard was established in 1989 and was originally intended to seek a wireless equivalent to Ethernet. In this way, it has developed successions of robust enterprise grade solutions that in many cases meet or even exceed the demands of the enterprise network. IEEE 802.11 wireless LAN networks are designed to provide wireless connectivity in a range of roughly 300 feet from the base. The lead application being shared over the wireless LAN is data. Provisions are being made to accommodate audio, video, and other forms of streaming multimedia.

Wireless security is a major demand in the secure data transferring services. Security challenges such as identity theft, international credit card fraud, communications fraud and corporate fraud are some of the main barriers preventing wireless technologies from growing and over taking the wired technology position. The 802.11b wireless LAN includes a protocol called wired equivalent privacy (WEP) which is meant to protect the wireless network.

We have been able to find some major flaws in this protocol which lead the whole system to be insecure and thus unreliable. For example, the cryptographic technique used in the WEP protocol, which is a fundamental tool to achieve the above goals, is rather primitive and can be broken fairly simply. The purpose of this paper is to explore the security vulnerabilities of the 802.11b wireless LAN and to present solutions for some of its major vulnerabilities.

Keywords: *Wireless Security, 802.11b Wireless LAN security, Cryptography*

1. INTRODUCTION

The trends and statistics suggest by the year 2005, 50% of fortune 100 companies will have deployed wireless LANs (source: Gartner Group). By year 2010, the majority of fortune 2000 companies will have deployed wireless LANs (source: Gartner Group). It's also predicted that there will be a significant increase in the use of wireless information appliances in the near future (e.g., PDA's, e-book) [1].

A major difference between wired and wireless networks is access to the transmitted data. In wired networks this is only possible by tapping the media used for the network where as in wireless networks since the media used is air, the transmitted data can be accessed by equipment that are readily available in the market for a cheap price. From the initial development stages of wireless technologies experts knew that security would be a major issue that needed to be solved in order for this technology to be able to overtake the place of wired networks.

One of the most popular wireless network standards being used today is the 802.11b wireless LAN standard. Around 2.2 billion dollars worth of 802.11b kits were sold in 2002. This standard includes a protocol called WEP (Wired Equivalent Privacy) which is meant to protect the wireless network.

2. WEP AND ITS FUNCTIONALITY

2.1 WEP's security goals are

Access control: protecting the wireless network from unauthorized access.
Confidentiality: to prevent eavesdropping.
Data integrity: to prevent tampering with transmitted messages.

2.2 WEP's security flaws

Several major flaws in this protocol are introduced in this paper. These flaws lead the whole system to be insecure and thus unreliable. In order to identify these problems we first need to understand how WEP intends to achieve its goals. WEP relies on an encryption algorithm called *RC4*. This algorithm works as follows:

CCECE 2004- CCGEI 2004, Niagara Falls, May/mai 2004
0-7803-8253-6/04/$17.00 ©2004 IEEE

2.2.1 At the sender the checksum of the message (which is the unencrypted data that needs to be transmitted) is calculated and the result is concatenated to the end of it. The result of this stage as can be seen in figure 1 is called the Plain Text.

2.2.2 A key stream is generated based on two fields:

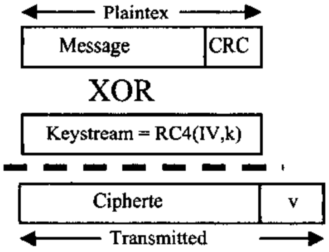
A secret key called k which is agreed upon by the hosts and servers of the network and is hard coded in them during the original set up of the network. Usually this key does not change for long a time, sometimes as long as the life of the network

A public key called *IV* which is dynamically generated upon encryption and is publicly available to all authorized and non authorized users.

2.2.3 The result of step 1 is XOR-ed with the result of step 2 which will create a bit stream called "*Ciphertext.*" This is illustrated in figure 1.

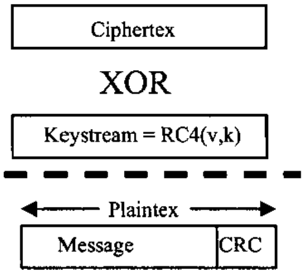
2.2.4 Then the Ciphertext which is the encrypted version of our original packet is concatenated with the IV field and transmitted. The reason the IV field is sent without any encryption is because it is a public key which is needed for decryption purposes by the receiver. This is not contrary to the structure of the algorithm since the IV field is a public key. The secret key k is the key that needs to be broken for an attacker to be able to decrypt data.

Figure 1: WEP Encryption (sender)



When the receiver receives the message it reads the IV transmitted with the message and based on it and also the secret key "k" which was hard coded into it at the set up stage of the network, it generates a key stream. This key stream is identical to the key stream generated at the receiver side since the same k and IV were used to generate both of them. Then it XORs this generated key stream with the transmitted Cipher text. This can be seen in figure 2. This will cancel out the key stream used in the encryption process leaving the original unencrypted plain text as the result [1].

Figure 2: WEP decryption (receiver)



The IV is only 24 bits long which will inevitably lead to key stream reuse. After a period of time the sending node will exhaust all possible values of the IV. After this stage the sending node will have no other choice but to use a previously used IV to generate the key stream. Thus two packets will be encrypted using the same k and IV. We will see in the following section that key stream reuse is a major vulnerability.

2.3 Key Stream reuse

Encryption in the RC4 algorithm is done based on two fields: the secret key k and the public key IV. Since the secret key k is constant, if the same public key IV is used to encrypt two packets then the two packets have been encrypted in exactly the same way. This is called key stream reuse. Two encrypted packets which were encrypted using the same key stream can be XOR ed to cancel out the two key streams. The result will be the XOR of the two original unencrypted packets. If the bit stream in one of the packets is known, it will give away the bit stream of the other packet and thus give away the secret key k. Usually only part of the bit stream of one of the packets can be guessed, in which case it wont give away the secret key k straight away but will give clues to solve it. This will help in obtaining k after several such incidences. One example of partial knowledge of the contents of a packet is acknowledgment packets which are very frequently used in TCP/IP networks. After the secret key k is obtained the encryption of the whole network is literally broken since the k is rarely changed after the set up of the network. At this stage the attacker will be able to decrypt all the messages being transmitted in the network.

In a typical busy network all possible IV combinations are used after about a day. In many cases the situation is even worse since many wireless network cards have poor IV management, for example some of them set the IV to zero every time they are initialized. A software called "Airsnort" which is available free of charge on the internet listens to all the traffic being transmitted across the wireless network. It looks for packets that have been encrypted using the same key stream (using the same IV). It calls them "interesting packets". After gathering a couple of hundred to a couple of thousand interesting packets it uses the clues it has gathered from all of them to break the secret key "k" of the network. The time it takes to break this key varies significantly usually based on how busy the network is [2].

3. SOLUTION TO THE KEY STREAM REUSE VULNERABILITY

Several possible solutions have been introduced to fix the security vulnerabilities of WEP. Most companies have tried to fix these security issues by increasing the size of the secret key k from an original 40 bits to 104 bits (called "128 bit" in the commercial market). Although this solution helps, it does not solve the core problem which is the reuse of the IV field. It should be noted however that this solution does have some benefits and as a result the infiltration of the network by an attacker would be more difficult. The main reason for this is because the key is longer in length and thus harder to solve using clues. Although it should be noted that this will only make the encryption breaking process longer, meaning that the attacker has to collect more "interesting packets" before it can solve k.

Another solution proposed recently by the WiFi Alliance is the WiFi Protected Access (WPA) which after testing looks very promising. WPA is a software upgrade for 802.11b/g LAN cards and routers. WPA solves the problem by doing two things:

3.1 Increasing the size of the IV field

WPA Increases the size of the IV field from 24 bits to 48 bits. Although this might seem a modest improvement initially, in reality it is increasing the possible IVs values from 16.7 million to about 281 trillion. This will decrease the likelihood of key stream reuse significantly.

3.2 Making the secret key k dynamic

Another improvement is making the secret key k dynamic so before the attacker has enough time to gather information to break the key, the key is changed. This is also a significant improvement since the original static key implementation was inherently vulnerable.

The dynamic key used in WPA changes after a certain period of time has elapsed (usually 10s-100s) or after a certain number of packets is transmitted (usually 10k packets). These changes are made based on a protocol called the Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA is compatible with most 802.11g and 802.11b wireless LAN cards. Although it is a recommended protocol in the new 802.11g standard, most vendors have not implemented it and instead have the upgrade available on their support websites. WPA will be mandatory in the upcoming 802.11i standard [3].

4. CONCLUSIONS

Wireless Technology has grown tremendously during the past few years. One of the major issues which needs to be addressed in order for this technology to replace the wired industry, is security. The 802.11b which is one of the most popular wireless network standards has a protocol called WEP in order to achieve equivalent security to wired networks. WEP only provides a margin of security since the encryption algorithm it relies on is vulnerable to attacks. Tests conducted by the authors came to the conclusion that the penetration of the 802.11b wireless network is possible using minimal equipment.

Many solutions have been introduced to fix the security issues of the 802.11b standard, the most common of these being the increase in the length of the secret key k. Although this solution makes the penetration process harder, it does not solve the main root of the vulnerability which is the reuses of IV numbers to generate key streams. One promising solution that was examined in this paper is a software upgrade called WiFi Protected Access (WPA) which has recently been introduced by the WiFi alliance. This protocol solves the root cause of the vulnerabilities by increasing the IV length and also changing the secret key k from a static key to a dynamic key.

Acknowledgements

We would like to acknowledge Professor David Falconer of Carleton University for his support and assistant with our fourth year project on wireless security. Also we would like to thank Carleton Student Engineering Society (CSES) for providing funding for participation in this conference.

References

[1] Christian Barnes, Tony Bautts, Donald Lloyd, Eric Quellet, Jeffery Bosluns, David M. Zendzian, and Neal O'Farrell (technical editor), *Hack Proofing Your Wireless Network.* USA: Syngress Media, 2002

[2] Matthew Gast, "Seven security problems of 802.11 wireless" An AirMagent Technial White Paper, http://www.fewireless.com/wireless/wlan_library/am_tech.pdf, December 2002

[3] Brandon Brown, "802.11: the security differences between b and i" *IEEE Potentials*, Vol. 22, No. 4, pp. 23-27, October/November, 2003