

# Weaknesses of Authentication and Encryption Methods Used in IEEE 802.11b/g Wireless Networks

Mohamed A. Saleh

Electrical Engineering Department, Faculty of Engineering,  
Alexandria University, Alexandria 21544, Egypt

Email: m\_saleh@ieee.org

**Abstract**— Recently, Wireless networking has become incredibly attractive to businesses and home users because of its flexibility. As WLANs become more widely deployed, wireless security has become a serious concern for an increasing number of organizations. WLANs attracted the attention of the cryptographic community, who rapidly detected cracks in some security approaches. This paper analyzes some flaws in the security aspects of the different 802.11 specifications, considering data confidentiality, integrity, mutual authentication, and availability. We will present some severe attacks against WLANs that violate wireless security and privacy.

**Keywords** — WLAN Security, WEP vulnerabilities, 802.11i flaws, DoS Attacks.

## I. INTRODUCTION

Conventional Internet users have been bound to wired connections. Wireless communications, however, have broken this restriction and provided unlimited access to the Internet. Today, the deployment of WLANs is sometimes even more economical and efficient than installing wired networks in a whole building.

In 1997, the IEEE standardized the 802.11 standard. This was the first WLAN standard accepted by multiple vendors as a true industry standard. The 802.11 standard has a maximum data transfer rate of 2 Mbps. This delayed the deployment of wireless networks especially with 100 Mbps networks on the market and 1 Gbps networks less than a year away. There was a need for greater bandwidth than what was available with the 802.11 standard.

In 1999, the IEEE group successfully standardized the 802.11a and 802.11b standards. 802.11a radios transmit at 5 GHz and send data up to 54 Mbps, whereas 802.11b radios transmit at 2.4 GHz and send data up to 11 Mbps. The higher operating frequency of the 802.11a leads to relatively shorter range as compared to 802.11b. The most widely available and implemented wireless LANs today comply with the 802.11b standard. In 2003, the IEEE approved the 802.11g standard. It is capable of a bandwidth of 54 Mbps and can support 802.11b clients. The 802.11g standard is very close to 802.11b from a coverage aspect.

Generally, the security requirements for a WLAN include data confidentiality, integrity, mutual authentication, and

availability. In order to provide data confidentiality equivalent to a wired network, the IEEE 802.11 Standard [14] originally defines Wired Equivalent Privacy (WEP) which is a scheme to secure IEEE 802.11 wireless networks. Several serious security weaknesses were identified in WEP. A WEP connection can be cracked with readily available software in one minute or less.

After the many problems with the security built into the WEP standard, a new security mechanism was needed to be developed, a new standard called IEEE 802.11i was developed. The 802.11i imply stronger encryption, authentication, and key management strategies that guarantee data confidentiality and system security.

The remaining of the paper is organized as follows. Section II discusses WEP and its vulnerabilities. Section III provides a general introduction to the enhanced security protocol IEEE 802.11i and outlines some of its known flaws. The key conclusions that can be drawn from this paper are stated in section IV.

## II. WEP THREATS

WEP relies on a secret key that is shared between a mobile station (e.g. a laptop) and a base station (i.e. an access point). Every transmission from a device on the LAN contains its MAC address so the identity of the sender can be checked. But how do we know that someone else did not forge a message with a fake MAC address. One approach is to agree to a secret code that will be used to protect every subsequent message. Because only the true device and the access point know the secret code, each message can be validated as authentic when it is received. The secret key is used to encrypt packets before they are transmitted and to decrypt them when they are received as well.

The original key length was 40 bits, which most manufacturers have increased to 104 bits. There is a problem in using a fixed key value because if an attacker spots the same encrypted bytes, he knows that the original plaintext is being repeated. The solution to this problem is the initialization vector (IV). Instead of just using the fixed secret key to encrypt the packets, the secret key is combined with a 24-bit number that changes for every packet sent. This extra number is called the IV and effectively converts the 104-bit key into a 128-bit key. Because the IV value always changes, the key used for

encryption effectively changes with every packet so even if the input data (plaintext) is the same, the encrypted data (ciphertext) is always different.

WEP uses a stream cipher called RC4 to encrypt the data packets. When the frame is ready for encryption, the system must select an IV value and append it to the secret WEP key. Once the IV and WEP key are combined together, the RC4 cipher is used to produce a pseudorandom number called "keystream". Before transmission takes place, WEP combines the keystream with the plaintext through a bitwise XOR process, which produces ciphertext (encrypted data). Fig. 1 shows the RC4 algorithm.

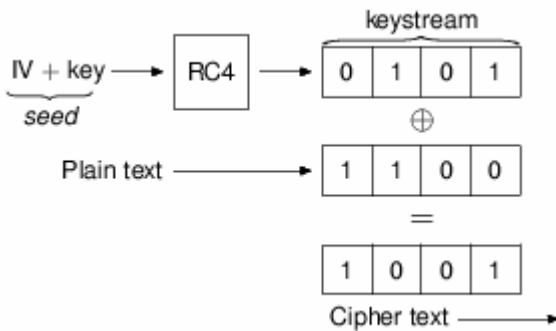


Figure 1. RC4 algorithm

In fact, the IV is not a secret. It is sent unencrypted as part of the transmission so the receiver knows which IV value to use in decryption as shown in Fig. 2. The receiving station uses this IV along with the shared secret key supplied by the user to decrypt the encrypted portion of the frame body.

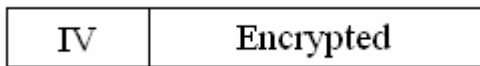


Figure 2. IV is sent unencrypted

To be effective, the same IV value should never be used twice with a given secret key.

From the Link Layer of a WLAN, there are three possible types of frames: Management Frames, Control Frames, and Data Frames. Any manipulation of these frames that directly or potentially jeopardizes data confidentiality, integrity, mutual authentication, and availability will be considered a threat. In this section, we outline some forms of attacks that WEP suffers from.

#### A. Illegitimate Authentication

When the mobile device requests authentication, the access point sends a random 128-bit number called challenge text. The mobile device then encrypts this number with the secret key using WEP and sends the result back to the access point.

Because the access point remembers the random number previously sent, it can check whether the result sent back was encrypted with the correct key. So any one watching this transaction now has the plaintext challenge and the encrypted response. Therefore, simply by XORing the two together, the enemy has a copy of the secret random bytes. The attacker now knows the keystream corresponding to a given IV value. Now the attacker simply requests authentication, waits for the challenge text, XORs with the previously captured keystream, and returns the result with the previously captured IV. The attacker is "authenticated" without ever knowing the secret key. Not only does this approach enable an attacker to authenticate, it actually assists him to attack the encryption keys.

#### B. Passive Attack to Decrypt Traffic

Because the attacker can read the IV value, he could keep a log of the values used and notice when a value is used again. Unfortunately the IV in IEEE 802.11 WEP is only 24 bits long. A 24-bit number has values from 0 to 16,777,216. So there are about 17 million IV values possible. A busy access point, which constantly sends 1500 byte packets at 11 Mbps, will exhaust the space of IVs after 5 hours, as in (1).

$$\frac{1500(\text{bytes}) * 8}{11(\text{Mbps})} * 2^{24} \cong 5\text{hours} \quad (1)$$

A passive eavesdropper can intercept all wireless traffic until an IV collision occurs (two packets with the same IV). This allows an attacker to collect two ciphertexts that are encrypted with the same keystream and perform statistical attacks to recover the plaintext. By XORing two packets that use the same IV, the attacker obtains the XOR of the two plaintext messages. Say we send messages A and B of the same length, both encrypted using same keystream K, So the attacker now has a message that is the XOR of two plaintexts as in (2).

$$\underbrace{(A \oplus K)}_{\text{Encrypted Message A}} \oplus \underbrace{(B \oplus K)}_{\text{Encrypted Message B}} = \underbrace{A \oplus B}_{\text{XOR of the two plaintext Messages}} \quad (2)$$

The attacker can look for more collisions of the same IV. With only a small amount of time necessary, it is possible to recover a modest number of messages encrypted with the same keystream, and the success rate of statistical analysis grows quickly. Once it is possible to recover the entire plaintext for one of the messages, the plaintext for all other messages with the same IV follows directly. Over time, the attacker can build up a table of IVs and corresponding keystreams, once it is built, the attacker can decrypt every packet that is sent over the wireless link.

#### C. Active Attack to Inject Traffic

WEP has a mechanism to detect whether any bits have been corrupted during transmission. All the bytes in the message are

combined in a result called the integrity check value (ICV). Even if a single bit in the message is corrupted, the receiving device will notice that the ICV value does not match and reject the message. The method used to compute the ICV is called a linear method. It turns out that one can predict which bits in the ICV will be changed if you change a single bit in the message. So if an attacker flips the value of a certain bit in the data, he can keep the ICV valid by also flipping a certain combination of its bits.

### III. IEEE 802.11i

IEEE 802.11i was designed to provide enhanced security in the Medium Access Control (MAC) layer for 802.11 networks. It was assumed that the new solution would completely replace WEP over time. The first and most important change in approach was the separation of the user authentication process and message protection.

The 802.11i defines a new type of wireless network called a robust security network (RSN). Unlike with WEP, in RSN there are many different keys, and most of these keys are not known before the authentication process completes. The creation of these keys is done in real time, that is why they are referred to as temporal keys. These temporal keys may be updated from time to time, but they are always destroyed when the security context is closed. There are two types of keys: a master key that provides authentication, and any number of temporal keys that are created or derived from the master key for use in decrypting unicast, multicast and broadcast traffics.

The 802.11i uses a number of standards, protocols, and ciphers which are either defined inside the 802.11i or have already been defined outside it. One of these standards defined outside the 802.11i is the IEEE 802.11x [15]. Its purpose is to implement access control. It divides the network universe into three entities: Supplicant, which wants to join the network (e.g. a laptop), Authenticator, which controls access (i.e. an access point), and Authentication server, which makes authorization decisions according to a list of allowed users. The authenticator acts as a sort of middleman in the authentication process, just relaying messages between the supplicant and the server until the authentication process completes.

Another standard used in 802.11i is EAP (Extensible Authentication Protocol) [18]. EAP is an authentication framework, not a specific authentication mechanism. EAP is designed to allow different types of authentication mechanisms to be used between the supplicant and the authenticator. Such mechanisms are called EAP methods and there are currently about 40 different methods including MD5, OTP, GTC, TLS, IKEv2, SIM, AKA and a number of vendor specific methods.

Having obtained the identity of the supplicant, the authenticator needs to contact the authentication server to find out whether this supplicant is to be allowed in. The authentication server can not make this decision until it has verified that the supplicant really corresponds to the identity it

has given. In effect, during this phase the supplicant and the server are talking directly. During the authentication process, the authenticator takes a quick look at each message that is passed between the supplicant and authentication server. It is watching for certain messages that it understands. In particular, it is looking for an EAP-Success or an EAP-Failure. It must wait until the authentication server indicates whether the supplicant has been accepted or rejected. When the authentication server makes a decision, the result gets sent to both the authenticator and the supplicant. This enables the authenticator to either allow access or disconnect the unauthorized user.

Although the 802.11i appears to provide effective data confidentiality and integrity, satisfactory mutual authentication and key management, there are some potential implementation oversights that may cause severe problems. We will focus on these problems.

#### A. SSID Spoofing Vulnerability

A service set identifier (SSID) is a code attached to all packets on a wireless network to identify each packet as part of that network. All wireless devices attempting to communicate with each other must share the same SSID.

The 802.1x protocol had experienced a number of vulnerabilities when the industry decided to adapt it to wireless. The protocol was originally used for wired port-based authentication, not wireless.

The general 802.1x vulnerability is achieved by setting up a rogue access point and getting clients to authenticate to this rogue access point. When these clients connected and passed their credentials, the attacker would use those credentials to connect to the actual network. The process involves sniffing the airwaves to find the SSID. It is easy because some frames have cleartext easy-to-read SSID.

First, an attacker needs to set up a server and an access point to use as a rogue device. The server needs to run on a laptop for portability, it also needs to run the following services: DHCP, DNS, and Web Server. Next, the attacker will need to set up the access point to use the same SSID as the target. This will allow any wireless device to connect to the attacker's wireless network if the attacker's signal is stronger. Once this happens and someone connects to it, a screen pops up asking if they want to connect to this network even though it is not secure. This may turn off the first user and make him think about it; however, given time and the number of users getting this screen, someone will just click OK. It does have a familiar-looking SSID that they are accustomed to.

Finally, someone connects and associates to the attacker access point. Now that the user is connected, the DHCP server on the attacker's station will serve up an IP address. Now the user is going to try to connect to some kind of network service or resource. Once the Web attempt is made, a DNS request will

be sent to the default gateway for the DNS server. The attacker will take the request and respond with his Web server's IP address as the page the user was requesting. Now the user will be directed toward the attacker's Web server without even knowing it. Once the Web page opens, a piece of Java script will launch that pop up a window. This window will look just like the default 802.1x authentication windows that the user has seen previously. Now the user will type in his username and password. Once he hits the OK button, the form is sent back to the attacker along with the user's full credentials. Now the attacker turns off his access point and the user connects back to his original access point and re-authenticates. Now the attacker can break in as a valid user without attempting any password guessing or brute forcing.

### B. Denial-of-Service (DoS) Attacks

IEEE 802.11i appears not to emphasize availability as a primary objective, leaving many DoS vulnerabilities even if the strongest data confidentiality and authentication protocols are used. Prior research has found numerous DoS attacks on a WLAN from the Physical Layer to the Application Layer.

802.11 networks utilize frames to manage connection and disconnection of stations from a wireless network. These are appropriately called management frames. One type of management frame, a deauthentication frame, is used to deauthenticate a station from a wireless network and may be sent by a station or an Access Point. Another type of management frame, a disassociation frame, is used to disconnect a station from a wireless network. Since the management frames are unprotected in a WLAN, an adversary can easily forge these frames to launch a DoS attack.

Among the management frame attacks, the most efficient attack is to forge and repeatedly send Deauthentication or Disassociation frames. It is also possible to target an entire wireless network by sending the deauthentication frames to the broadcast address instead of directing them to an individual station.

Also There are several DoS attacks that exploit the unprotected EAP messages in 802.1X authentication. When a device wishes to connect to an 802.1x authenticated network, it must send an EAP-Start message to the Access Point to initiate the authentication process. This causes the Access Point to allocate some resources for the authentication transaction. Thus, an attacker can flood the Access Point with EAP-Start messages and cause it to exhaust its resources and disrupt wireless LAN service. An adversary also can forge EAP-Start messages repeatedly to prevent the 802.1X authentication from succeeding as well as forging EAP-Failure message to disconnect the supplicant.

Also when a station wishes to leave a WLAN it will send an EAP-LogOff message to the Access Point to end its authenticated session. Therefore it is possible for an attacker to

spoof the MAC address of an authenticated station and send an EAP-LogOff message to the Access Point. This will cause the Access Point to believe that the legitimate station has really ended its legitimate session.

## IV. CONCLUSIONS

Our results demonstrate serious flaws in all of the security mechanisms used by WLANs supporting the IEEE 802.11 wireless standard. We recommend that anyone using an 802.11 wireless network not rely on WEP for security, and employ other security mechanism to protect their wireless network. Although the emerging IEEE 802.11i standard could potentially improve security services in today's IEEE 802.11 WLANs, it is expected that more work is needed to develop a more secure WLAN environment. All of these attacks are practical to mount using only inexpensive equipments. The end result is that all of the deployed 802.11 wireless networks are at risk of compromise.

## ACKNOWLEDGMENT

We thank John Walker for his interest and feedback. We are indebted to M. Ramadan, who provided many valuable comments.

## REFERENCES

- [1] J. Edney and W. Arbaugh. Real 802.11 Security: Wi-Fi Protected Access and 802.11i. Addison Wesley, July 2003.
- [2] C. Peikari and S. Fogie. Maximum Wireless Security. Sams Publishing, December 2002.
- [3] T. M. Swaminatha and C. R. Elden. Wireless Security and Privacy: Best Practices and Design Techniques. Addison Wesley, September 2002.
- [4] B. Fleck and B. Potter. 802.11 Security. O'Reilly, December 2002.
- [5] J. C. Chen, M. C. Jiang and Y. Liu, "Wireless LAN security and IEEE 802.11i", IEEE Wireless Communications, Volume 12, No. 1, pages 27 – 36. February, 2005.
- [6] R. K. Nichols and P. C. Lekkas. Wireless Security Models, Threats, and Solutions. McGraw-Hill professional, December 2001.
- [7] N. O'Farrell, E. Ouellet, and E. Ouellet. Hack Proofing Your Wireless Network. Syngress, February 2002.
- [8] L. Barken. How Secure Is Your Wireless Network? Safeguarding Your Wi-Fi LAN. Prentice Hall PTR, August 2003.
- [9] NIST, Special Publication 800-48, "Wireless Network Security:802.11, Bluetooth and Handheld Devices", November 2002
- [10] C. He and J. C. Mitchell, "Security Analysis and Improvements for IEEE 802.11i", The 12th Annual Network and Distributed System Security Symposium (NDSS'05), pages 90-110, Feb. 2005.
- [11] M. S. Gast. 802.11 Wireless Networks: The Definitive Guide, O'Reilly, 2002.
- [12] S. McClure, J. Scambray, and G. Kurtz, Hacking Exposed: Network Security Secrets & Solutions, 4th ed., McGraw Hill/Osborne, 2003.
- [13] W. A. Arbaugh, N. Shankar, and J. Wang. Your 802.11 Network has no Clothes. In Proceedings of the First IEEE International Conference on Wireless LANs and Home Networks, pages 131-144, December, 2001.
- [14] IEEE Standard 802.11-1999. Information technology Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control and Physical Layer Specifications. 1999.
- [15] IEEE Standard 802.1X-2001. IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control. June, 2001.
- [16] M. Lynn and R. Baird. Advanced 802.11 attack. Black Hat Briefings, Las Vegas, NV, July, 2002.
- [17] J. R. Walker. Unsafe at any key size; An analysis of the WEP encapsulation. IEEE Document 802.11-00/362, October 2000.
- [18] L. Blunk, J. Vollbrecht. Extensible Authentication Protocol (EAP). Internet Draft draft-ietf-eap-rfc2284bis-06.txt, September 2003.