Today & Tomorrow: IEEE 802.11 WLAN Security

L. Ertaul[1]**, O. Catambay**[2]
[1]Department of Mathematics and Computer Science, California State University, East Bay, Hayward, CA, USA,
Levent. Ertaul@csueastbay.edu
[2]Department of Mathematics and Computer Science, California State University, East Bay, Hayward, CA, USA,
ocatambay@horizon.csueastbay.edu

Abstract - *After all those enhancements in Internet technology, the Internet has become part of people's lives, so they want to have it ready to use not only on their PCs but also in their mobile devices. WLANs have become very popular thanks to the development of IEEE 802.11 standard family. As wireless applications and systems are widely adopted wireless security is becoming increasingly important. Wireless security is different then wired security primarily it gives potential attackers easy medium access. And the future of WLANs depends on successful deployment of security techniques in these systems. In this paper we are discussing the current and future security concerns of 802.11 protocols family and based on this discussion we are addressing achievability of complete security in future WLANs.*

Keywords: Wireless Security, IEEE 802.11, WEP, WPA, TKIP, CCMP

1 Introduction

Let the battle for supremacy begins: Wired Local Area Networks versus Wireless Local Area Networks (WLANs). No doubt arguments can be made to support either one, however, if one was to ask which technology will win out in the 21st century, which technology will revolutionize networking infrastructures, and which technology captures the imaginations of networking professionals and the mundane American, no doubt wired is the past, and wireless is the present and the future.

But in order for wireless to dominate the networking world skeptics of wireless technology argue that two things must happen: (1) Throughput must match and surpass that of wired networks, and (2) Security must be guaranteed, if not it must be made extremely difficult to breach.

Although the significance of throughput should not be ignored, we will do so here in favor of discussing the security aspects of WLANs.

In addition, numerous questions arise regarding WMDs. No, not President Bush's fictitious WMDs, but Wireless LAN—Mass Deployments. Thus, we will attempt to answer the following questions regarding the mass deployments of WLANs:

- Can WLANs become completely secure?
- Can organizations that handle private customer information such as *banks*, hospitals, and government agencies, integrate WLANs within their wired network infrastructures without compromising private/sensitive information?
- What does the future hold for WLANs?
- Will WLANs make wired-networks obsolete?
- Can WLANs become commercially successful?

Moreover, we will also address the security issues associated with the IEEE 802.11 WLAN Family of standards. In particular, we will investigate the failures of the Wired Equivalent Privacy (WEP) protocol, discuss proposed countermeasures by industry leaders, and introduce the enhancements being worked on by Task Group I of the IEEE 802.11 standard which is in the end-process of ratification. Finally, we will discuss tomorrows of WLAN security.

2 The IEEE 802.11 WLAN Family of Standards

The birth of WLANs took place on October 1997 with the ratification of the IEEE 802.11—legacy standard, which defined the medium access control (MAC) and physical layers of WLANs. In particular, two physical access methods using radio frequency transmission were designated: Frequency Hopping Spread Spectrum (FHSS), and Direct Sequence Spread Spectrum (DSSS) which operated within the Industrial, Scientific, Medical (ISM) band spectrum (2.4 GHz) [1], [2].

In 1999, IEEE released two sub-standards aimed at improving the medium access control and physical layers, 802.11a and 802.11b. 802.11a uses an alternate unlicensed band—the 5.0 GHz unlicensed national infrastructure (UNII) band, which in turn uses a coded multi-carrier mechanism called orthogonal frequency division multiplexing (OFDM). 802.11b uses the same ISM band as 802.11-legacy with

DSSS and is therefore backwards compatible with 802.11-legacy products. In 2003, IEEE introduced a new standard 802.11g which is notably referred to as “802.11b-extended” in that it is compatible with 802.11b. 802.11g differs from 802.11b in that it uses OFDM and offers a greater maximum physical layer rate of up to 54 Mbps compared to 11 Mbps of 802.11b [1], [2], [3], [4], [5].

More enhancements/amendments were made on 802.11-legacy which we will list here [4]:

- 802.11c and 802.11d: Covers additions concerning bridging support and includes updates for physical layer requirements (if deployed outside U.S)
- 802.11e (MAC Enhancements):This substandard works to provide QoS for WLANs and applies to all 802.11 standards. It will also work to link wired Ethernet QoS (802.1p) and WLANs.
- 802.11f (Inter-Access Point Protocol):Aimed to resolve problems arising when roaming between Wirelesses Access Points (APs) deployed by different vendors and standardizes necessary exchange of information amongst APs to support functionalities of a distribution system (i.e. sharing of resources).
- 802.11h (Spectrum managed 802.11a): Considers European requirements for power control and dynamic selection of transmit frequency and allows 802.11a products to be deployed in Europe.

This leads us to 802.11i, which targets at improving the current security scheme of 802.11 products called Wired Equivalent Privacy Protocol (WEP) [6], [7]. But before we discuss the security enhancement standard, let us investigate what the current WLAN security protocol WEP is, and why it failed at meeting its goals.

3 Today–The Goals of Wired Equivalent Privacy (WEP)

As stated earlier, WEP is the current security protocol used by current 802.11 products. It has two goals in mind: (1) to provide security equating the security schemes of wired LANs, and (2) to protect MAC protocol data units (MPDU) [8], [9].

WEP uses a default key and the RC4 [10] algorithm to encrypt MPDUs. The default key can be either a key shared between an access point (AP) and more than one node, or a key-mapping key, which is a key shared between an AP and only one other station [9], [11], [12].

In turn, the RC4 algorithm functions as a pseudo-random number generator (generating a per-packet key) which accepts a 24-bit initialization vector (IV) concatenated with a key to make a per-packet key.

Furthermore, WEP uses CRC-32 to compute an Integrity Check Value (ICV) on the MPDU. The resulting 32-bit ICV is attached to the end of the MPDU before being encrypted. The MPDU and ICV is encrypted by XOR-ing it with the per-packet key. The IV and a key ID is then attached in front of encrypted MPDU which makes our WEP Protocol data unit—our cipher-text [9], [11], [12]. Fig. 1 illustrates the WEP protocol data unit and Fig. 2 shows how WEP works:

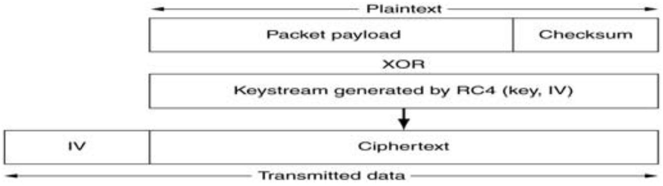

Figure. 1. WEP protocol data unit

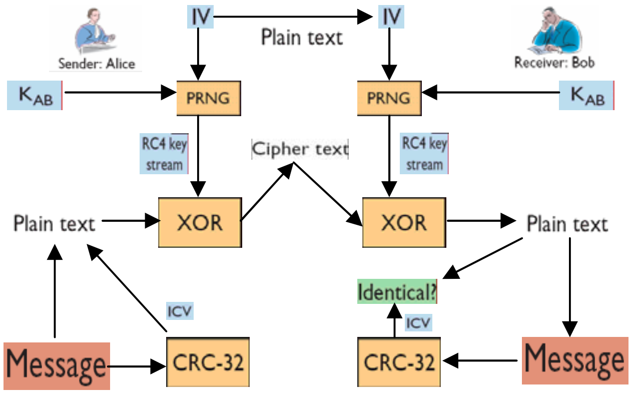

Figure. 2. How WEP works.

3.1 The Failures of WEP

We can categorize the failures of WEP into poor physical implementations and policies by IT professionals and poor cryptographic implementations standardized by protocol developers.

3.1.1 The Failures of WEP protocol Implementation

The implementers of WEP used a weak implementation of the RC4 symmetric algorithm. That is, due to its short implementation lengths, WEP keys are easily obtained by cryptanalysis [11], [12]. Thus, with enough “snooped” packets it is easy for a cryptanalyst to retrieve the key.

Another problem is WEP’s implementation of the Cyclic Redundant Check (CRC) -32 algorithm: It computes a non-cryptographic value that is vulnerable to “side-channel attacks". This in turn compromises the integrity of the data [9], [11], [12].

Even more, WEP's authentication scheme can also be breached. Whackers—wireless crackers [13], can spoof broadcasted MAC addresses since WEP broadcasts MAC addresses unencrypted. This can be accomplished by using a wireless Network Interface Card (NIC) configured with the sniffed MAC address. The consequence is thus critical in that a possible attacker can act as an authorized user of an organization's network [11], [12].

3.1.2 Failures of IT policies

For one, the default configurations of 802.11 deployed products (Bases Stations) are deployed with WEP disabled. Thus IT policies must ensure that WEP is enabled in their products. Although WEP is unable to provide complete security, with proper configuration, it does provide an enhanced form of WLAN security.

Also, network administrators must make sure that the default service set identifier (SSID) of the AP is changed. If it is not changed, an attacker simply finds out the default SSID of the specified vendor and thus can access to the network. The AP's broadcast mode must also be disabled, as not to broadcast the changed SSID.

The actual physical accesses to base stations must also be considered in WLAN deployments. APs should be located where possible attackers cannot reset the AP's to its default factory settings.

In addition, whackers can take advantage of the AP's coverage areas. Simply put, signals from the AP may go beyond the desired areas. For instance, signals can "bleed-over into parking lots where whackers can collect and analyze bled-over signals. This form of attack is known as "war driving" [13].

Hence, the general problems with WEP is that an attacker can easily eavesdrop plain-texts and cipher-texts over our wireless medium which in turn leads to an attacker obtaining the pseudorandom key stream produced by the RC4 algorithm. It is now reasonable for us to proclaim that WEP fails in meeting its inherent goal of wired-equivalent confidentiality and fails in meeting the expected goals for data integrity and user authentication. Thus, a new security scheme is desired [9], [11], [12].

3.2 Security Attacks on WEP

In August of 2001 Flurher, Mantin, and Shamir (FMS) showed how eavesdroppers can attack. Attackers are capable of obtaining several million encrypted packets whose 1st byte of plaintext is known. They can then deduce the base RC4 key by exploiting the properties of the RC4 key schedule. Within a week of FMSs publication, Stubblefield, Ioannidid, and Rubin (SIR) implemented the attack and thus demonstrated how real systems can be cracked. [8]

Other known WEP attacks include: (1) Jesse Walker, who showed how the small IV size creates risk of key stream reuse and allows eavesdroppers to recover plaintext; (2) Nikita Borisov, Ian Goldberg, and David Wagner, whom showed that encrypted messages can be modified and showed that user authentication an be trivially defeated; and (3) William Arbaugh, who showed how an attacker could decrypt any chosen packet in only a few hours [8], [14].

4 Alternatives to WEP

There exist three possible solutions to WEP. One solution was introduced in October 2002 by the Wi-Fi Alliance called the Wi-Fi Protected access (WPA). WPA is a proprietary security standard for WEP which substitutes WEP to provide enhanced security and interoperable services. The use of WPA will be forward-compatible with IEEE 802.11i [14].

IEEE's solution to WEP is 802.11i, which will offer 2 options. The first option is the short-term solution, aimed for already deployed products, Temporal Key Integrity Protocol (TKIP) [6], [7]. The second option is Counter-Mode-CBC-MAC Protocol (CCMP) which provides the long-term solution and is aimed towards developing products [8], [14].

Now let's have a look short-term and long-term solution to WEP in following sections.

4.1 802.11i—Temporal Key Integrity Protocol (TKIP): Temporary Solution (Short-Term)

TKIP is a set of algorithms that adapts the WEP protocol. It addresses WEP's known flaws while meeting constraints.

TKIP works by wrapping WEP into 3 new elements: (1) Michael: Message integrity code (MIC) to defeat forgeries. (2) Packet sequencing discipline, to defeat replay attacks. (3) Per packet key mixing function, prevents FMS attacks [6], [7]. Fig. 3 below shows how TKIP adapts WEP using these 3 new elements.

Furthermore, TKIP mandates fresh keys to address the vulnerability of reusing keys. TKIP accomplishes this by using IEEE 802.1x key management scheme. TKIP requires the use of two keys, a 128-bit key used by the mixing function, and a 64 nit-key used by Michael—MIC [8].

The basic idea behind the Michael message integrity code (MIC) algorithm is that it computes the keyed function of data at the transmitter. It sends the MIC code to the receiver as a tag with the data. The tag is recomputed and the value is compared to the accompanying data. Thus, if the tag matches the receiver authenticates the data, however, if there is no match a forgery of some sort has occurred, and thus the receiver rejects the data.

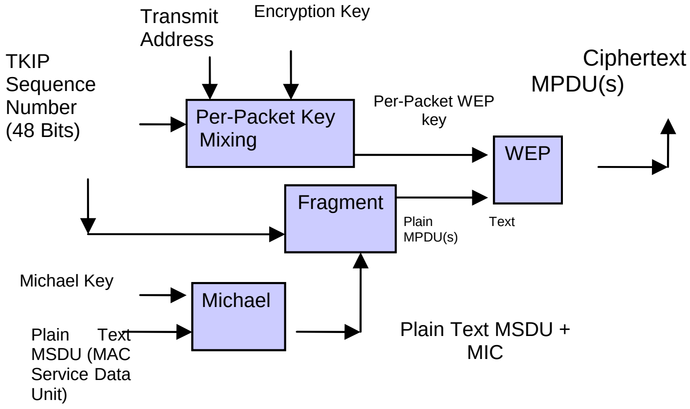

Figure. 3. How TKIP works

Michael works by using a 64-bit key and partitioning the packets into 32-bit blocks. It then uses shifts, XORs, and additions to process each 32-bit block into 32-bit registers that will represent the final output which is our 64-bit authentication tag.

Packet Sequencing is aimed at addressing the problem of replayed packets. It solves the problem by binding packet sequence number to each packet with the MIC code. This in turn enforces packet sequencing at the receiver. Reinitialization of the sequence space is thus mandated whenever the MIC key is replaced.

As we stated earlier, TKIP extends the current WEP format by using a 48-bit sequence number. It also associates each sequence number with the encryption key instead of MIC key.

TKIP introduces a new per-packet encryption key construction, which is based on a mixing function. This mixing function takes a base encryption key, transmitter MAC address and the packet sequence number as inputs. It outputs a new per-packet WEP key.

The Mixing function is split into 2 phases. The first phase uses a non-linear substitution table—S-box, which combines the base key, transmitter MAC address, the 4 most significant octets of the packet sequence number to produce an intermediate value. This intermediate value is then cached and used for up to 2^{16} packets and since transmitter address is included, the mixing function produces different values on each host even when base key is same with multiple hosts.

The second phase separates the packet sequence number from the per-packet key to help defeat FMS attacks. It mixes the intermediate value with the 2 least significant octets of the packet sequence number, which produces a per-packet key [8].

4.2 802.11i—Counter-mode-CBC-MAC Protocol (CCMP): Long-Term Solution

The long term solution provided by 802.11i uses the Advanced Encryption Standard (AES) [15], [16] as its encryption algorithm. However, since current AES modes of operation are ill-suited for WLAN operations, a new mode called Counter-Mode-CBC-MAC (CCM) has been established and thus submitted to the National Institute of Standards and Technology (NIST) for use as a Federal Information Processing Standard [8], [9], [14].

CCM mode merges 2 well-known and widely deployed techniques. The first technique is Counter Mode which is used for encryption and the second technique uses Cipher Block Chaining Message Authentication Code (CBC-MAC) for integrity protection. Both of these algorithms respectively uses only the encryption primitive at both sender and receiver endpoints. CCM also uses the same key for both confidentiality and integrity. The following figure illustrates the CCM mode:

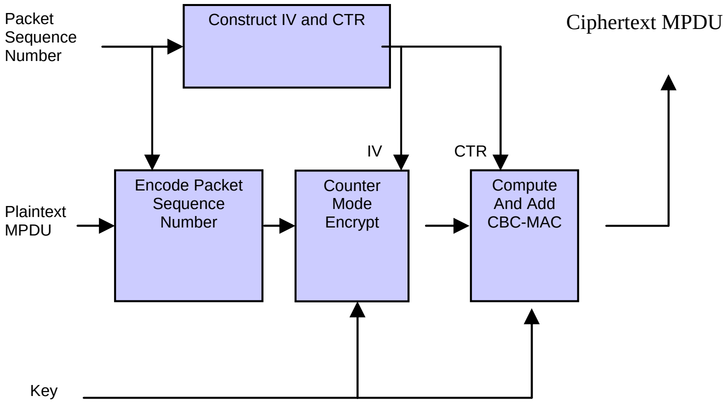

Figure. 4. CCM Mode

As previously stated, CCM protocol (CCMP) uses AES, which is arguably considered as the best choice amongst symmetric-key cryptographic algorithms and is therefore the best choice for the long term solution to WLAN security. AES uses a 128-bit key but does not require per-packet keys. It uses a 48-bit IV which in turn ensures that the AES key lifetime is longer than any possible association. CCMP also uses the 48-bit IV as sequence numbers to detect replay attacks

Furthermore, CCMP uses the same AES key to provide confidentiality and integrity protection for all packets in an association, and uses an 8-octet MIC. Also, unlike WEP and TKIP the encrypted ICV is no longer needed [8].

5 Tomorrows of WLAN Security

Let us now revisit and answer the questions we posted at the beginning of this paper.

First, WLANs cannot be completely secure, but through a collection of countermeasures, the use of new security standards, and ensuring that IT polices are practiced, adequate security can be achieved.

Second, WLANs can be used by organizations that handle private customer information such as banks, hospitals, and government agencies, can integrate WLANs within their wired network infrastructures without compromising private/sensitive information, but not as an extension of the wired network for now. They should instead be deployed outside of wired networks.

Thus, thirdly, we believe that the future of WLANs look bright. It is already deployed in coffee shops, bookstores, schools, grocery stores, airports, homes, and even WAL-MART!

Fourth, although WLANs will not make wired LANs obsolete, they work well together. WLANs complement wired LANs in that it provides user convenience through mobility.

And lastly, WLANs can become commercially successful because IEEE 802.11 WLAN creates the possibility for every imaginable device, to be a mobile device. The upcoming IEEE 802.11i Security Enhancement Standard will only make the deployments of WLANs more desirable! However, we must all realize that complete security is unrealistic, but a collection of policies and cryptographic algorithms combined will make the jobs of whackers and crackers alike more and more difficult.

6 Conclusions

We see a future where every human being on Earth owns a device where he or she can communicate securely with anyone, anywhere and anytime as if that person was in the same room, and all we are doing is yelling across the room using our own personal lingo or slang. IEEE 802.11 WLAN will thus serve as the backbone for this network of wireless devices or for that matter, function with no backbone at all. That is, a collection of 802.11-enabled products communicating ad-hoc-ly! Thus, the possibilities for applications appear endless and WMDs (WLAN Mass Deployments) are inevitable although completely secure WLANs are unrealistic. There are and will be possibilities to have a sound security for WLANs by a suitable integration of technologies, policies and standards.

7 References

[1] Heegard, C. et al.: "High-Performance Wireless Ethernet", IEEE Communications Magazine, pages 64-73, Nov. 2001

[2] Severance, C.: "IEEE 802.11: Wireless Is Coming Home", IEEE Computer, pages:126-129, Nov. 1999.

[3] Kapp, S.: "802.11: Leaving the Wire Behind", IEEE Internet Computing, pages 82-85, Jan.-Feb. 2002.

[4] Schiller, J.: "Mobile Communications" 2nd Edition. Addison-Wesley, 2003.

[5] Varshney, U.: "The Status and Future of 802.11-Based WLANs", IEEE Computer pages 102-105, June 2003.

678. 9. 10. 11. 12. 13. 14. 15. 16

[6] IEEE std. 802.11-01/550r3.: "Wireless LANs: Temporal Key Hash", IEEE Press, Dec. 2001

[7] IEEE std 802-11-02/282r2.: "Wireless LANs: Alternate Temporal Key Hash", IEEE Press, Apr. 2002.

[8] Cam-Winget, N., Russ H., David W, & Jesse W. : "Security Flaws in 802.11 Data Link Protocols.", Communications of the ACM, Vol. 46. No. 5. pg.35-39, May 2003

[9] Housley, R., Arbaugh, W.: "Security Problems in 802.11-Based Networks.", Communications of the ACM, Vol. 46. No. 5, pg. 31-34, May 2003

[10] Rivest, R.: "The RC4 Encryption Algorithm", RSA Data Security, March 1992.

[11] Park, J. S., Dicoi, D.: "WLAN Security: Current and Future", IEEE Internet Computing, pg.60-65, Sept.-Nov. 2003.

[12] Potter, B.: "Wireless Security's Future.", IEEE Security & Privacy, pg. 68-72, July/August, 2003

[13] McFedris, P.: "Hacking Unplugged.", IEEE Spectrum, pg. 80, Feb. 2004.

[14] Arbaugh, W. A.: "Wireless Security Is Different.", IEEE Computer, pg. 99-101, August 2003.

[15] Daemon, J., Rijmen, V.: "AES Proposal: Rijndael". http://csrc.nist.gov./encryptions/aes

[16] Federal Information Processing Standarts Publication (FIPS) 197.: "Advanced Encryption Standard (AES)." Nov. 2001.http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf