



---

# 802.11 Security

## Abstract

The standard security built into all 802.11 products today has been found to be vulnerable to attack both theoretical and practical in nature. The IEEE Task Group I has been working for the past two years to develop an security standard known as the Robust Security Network (RSN) which will address all known attacks and greatly improve the security of 802.11 based equipment. The significant features of RSN consist of IEEE 802.1X and two new encryption protocols to replace WEP. This paper describes several of the WEP attacks that have been identified to date and describes the 802.11i draft standard as it exists today. The paper concludes with a discussion on some of the common authentication protocols that will be used in conjunction with 802.11i in the enterprise environment.

## Introduction

Wireless local area networking (WLAN) technology based on the Wi-Fi (802.11) standard has brought great benefits to consumers in the enterprise, home, and public access markets. Wi-Fi provides a robust high speed connection to a network without the tether associated with a wired network. While the wireless technology provides great benefits for mobility and productivity, it also brings with it added requirement to employ security measures that are not always required in a wired network. Since Wi-Fi is based on radio frequency (RF) technology, the information transmitted over the wireless network is not constrained by most physical barriers.

Unlike a wired network, anyone with Wi-Fi equipment in proximity of the WLAN can connect to the network if the network does not employ security mechanisms to prevent them from doing so. Once connected to the network, an unauthorized user could do a number of things ranging from simply making use of a broadband connection to the internet, to accessing other resources on the network, to eavesdropping on network traffic, to malicious denial of service (DoS) attacks.

To further complicate the issue, the standard security built into today's 802.11 based equipment, Wired Equivalent Privacy (WEP), can be compromised by someone with the appropriate tools and expertise to do so. Although failure to use WEP is the primary security weakness, WEP is only effective as a deterrent for casual snoopers forcing users needing a highly secure solution to use other technologies (e.g. virtual private networks) or proprietary features to secure their WLAN.

---

The IEEE 802.11 Task Group I is close to finalizing an standard for improved security on 802.11 based WLANs called the Robust Security Network. The solution provides significant improvements in the authentication and privacy and addresses all of the issues associated with WEP in the original 1999 standard. It provides solutions for legacy 802.11 hardware as well as future Wi-Fi equipment that is expected start coming to market sometime in 2003.

To prevent unauthorized access to a WLAN, a robust security solution should provide strong mechanisms for authentication and privacy. Authentication refers to the process by which the identity of a device is verified prior to a network connection being completed. Mutual authentication should be employed to verify the identities on both ends of the connection. In this case the identity of the device connecting to the network (referred to as the client or station) is verified by the network and the identity of the network is verified by the client.

After mutual authentication, a connection between the network and the station is established and privacy mechanisms are employed to protect the data being sent over the wireless connection. Privacy involves encryption or scrambling of the data to prevent eavesdropping by unauthorized listeners. A good privacy mechanism will also include protection mechanisms to ensure that the data was not altered en route to the receiver and validate the addresses of the sender and receiver of the data. The aforementioned features are all elements of the Robust Security Network standard being created by the IEEE Task Group I.

## **WEP Encryption**

### **WEP Overview**

The original IEEE 802.11 standard published in 1997 included an optional privacy mechanism known as Wired Equivalent Privacy (WEP). As it's name implies, WEP was intended to provide a level of protection equivalent to that provided by a wired network connection. The goals of WEP as outlined in the standard were to be reasonably strong, self synchronizing, computationally efficient, and exportable. To accomplish these goals, the WEP protocol was designed to operate using the RC4 stream cipher with 40-bit encryption keys and a 24-bit initialization vector (IV). 40-bit encryption keys are specified by the standard, although 104-bit encryption keys have become a de-facto industry standard.<sup>1</sup>

A network which operates without WEP enabled is said to be an open network and a network utilizing WEP is a closed network. In an open network, any station requesting an association with the network is allowed to connect to the network. Furthermore, all communication inside the WLAN is also done in the clear and unencrypted. In a closed network, each station and access point (AP) on the network must be provided the encryption keys to be used to scramble the data. Only equipment with knowledge of these encryption keys are able to successfully encrypt and decrypt the data and thus participate in communication using the WLAN. A node transmitting data will encrypt the data using the shared WEP key prior to transmission of the data. A receiving node will

---

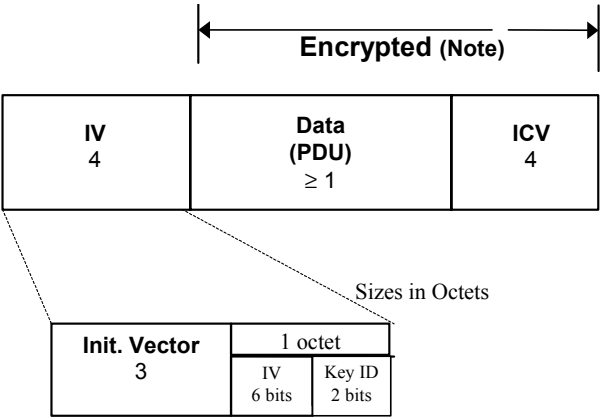
<sup>1</sup> A system using 104-bit keys will often be referred to as having "128-bit encryption". This is arrived at by combining the length of the shared key (104 bits) with that of the initialization vector (24-bits) for a total of 128 bits. This nomenclature, although commonly used, is inconsistent with the reference to 40-bit WEP as defined by the 802.11 standard. In the later case only the length of the shared key is referenced. For consistency, 128-bit WEP using a 104 bit shared key is analogous to 64-bit WEP using a 40-bit shared key.

use the shared WEP key to decrypt the data after it has been received and before passing it on to either the host computer or the wired network to which it is attached.

A major criticism of WEP has been that it does not provide a mechanism for the distribution of the encryption keys and assumes that they have been distributed in a secure manner to each of the network nodes through some other means. Typically, this means that the WEP keys have been distributed through manual means by users of the equipment or the administrator of the computer network. This reliance on manual key distribution has meant that WEP does not scale well for large deployments where distribution and management of the WEP keys can quickly become impractical.

**How WEP Works**

The format of the data portion of an WEP encrypted 802.11 frame (referred to as a MAC Protocol Data Unit or MPDU) is shown below in Figure 1.



**NOTE:** The encipherment process has expanded the original MPDU by 8 Octets, 4 for the Initialization Vector (IV) field and 4 for the Integrity Check Value (ICV). The ICV is calculated on the Data field only.

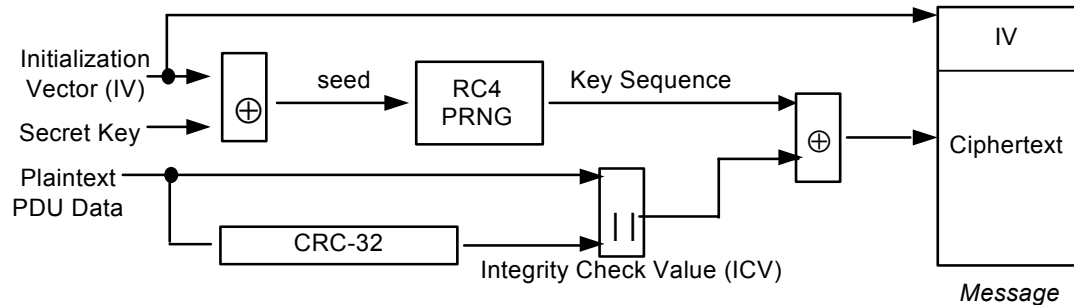
• Figure 1 – MPDU format using WEP encryption

As can be seen by the diagram, the original MPDU is expanded by 8 octets (bytes). Four octets (bytes) are added to the front of the PDU for the initialization vector (IV) and four octets are added to the end of the PDU to form an integrity check value (ICV). The four bytes comprising the IV are made up of a 24-bit initialization vector followed by 6 bits of padding and 2 bits that serve as the key ID<sup>2</sup>. The 24-bit initialization vector provides two functions in the WEP protocol; it is the mechanism by which a new encryption key is generated for each PSDU and it provides synchronization by keeping the encryption/decryption process synchronized in the case of lost or retransmitted packets. This is explained in further detail below. The ICV is a CRC-32 checksum performed over the unencrypted data (plaintext) and transmitted in the PSDU. The ICV allows the receiver to determine if the received packets was altered or tampered en route.

The WEP encapsulation process is shown below in Figure 2. The IV is concatenated with the static secret shared key (40-bit or 104 bits) to form the seed that is used to initialize the

<sup>2</sup> WEP allows for the use of four static keys in a basic service set (BSS). A station can transmit using only one of the four keys, but must be able to receive data on any of the four keys. The key ID identifies which of the four shared keys was used to encrypt the PSDU.

RC4 cipher. The IV should be unique for each packet and this is the recommended practice called out in the 802.11 standard. For many implementations this is simply a counter that increments for each packet. The RC4 cipher creates a random bit sequence that is combined in an exclusive or (XOR) operation with the plaintext to create the ciphertext included in the PSDU. The plaintext is created by concatenating the PDU data with the ICV formed from the CRC-32 of the PDU data. In the final operation the IV is prepended to the ciphertext and thus the IV is broadcast in the clear with each packet.



• Figure 2 – The WEP encapsulation process

## WEP Compromises

Starting late in 2000 a number of weaknesses of WEP were identified and published. Initially, the issues identified related to specific implementation weaknesses or primarily theoretical attacks on WEP itself. Later, a practical and efficient attack based on the known properties of the RC4 cipher used in WEP was outlined. The more relevant WEP issues are identified below.

### The University of California Berkley Paper

In 2000, a team of researchers from the University of California Berkley published a paper which outlined a number of weaknesses of WEP<sup>3</sup>, a number of which were due to specific vendor implementations rather than inherent weaknesses in WEP itself.

#### Keystream Reuse

Keystream reuse means that the same random data used to encrypt the cleartext is reused across multiple packets. With WEP this means that the same encryption key is used to encrypt multiple packets on the WLAN, either from the same station or from multiple stations. The IV described above is the mechanism used by WEP to avoid keystream reuse. If the same keystream is reused, over time, this can reveal information about the keystream thus eventually allowing an attacker to decrypt data sent over the WLAN.

The authors identified two weaknesses that can lead to keystream reuse. The first resulted from poor WEP implementations in which some vendors would either not update the IV or update it infrequently. The 802.11 standard recommends that the IV be updated with each packet. The second weakness resulted simply from the fact that the IV, being only 24 bits in length, can lead to reuse in as few as 5000 packets with only two stations

<sup>3</sup> "Intercepting Mobile Communications: The Insecurity of 802.11", [www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf](http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf).

on the WLAN sharing the same 40-bit WEP key. As more stations are added to the WLAN, this number of packets decreases.

### **Linear Message Integrity Check Function**

As was outlined above, the message integrity check function utilized by WEP is a simple CRC-32. By placing himself between the transmitter and the receiver of a message, an attacker can use this property to launch a denial of service attack. In this scenario, the attacker intercepts packets destined for the receiver and flips bits in the frame body. Since a simple CRC-32 is used, the attacker can also change the appropriate bits in the CRC to match the bits that were changed in the frame body. The frame is then forwarded to the receiver where the tampered message will be successfully decoded without any indication that the message was altered.

### **Unkeyed Message Integrity Check Function**

This weakness results from the fact that the message integrity check does not include any knowledge of the WEP key as part of its calculation. In this attack it is first assumed that the attacker has recovered the keystream by some method. Having done this, the attacker can successfully inject messages into the BSS by encrypting them with the keystream and then calculating and attaching the appropriate CRC-32 to match the encrypted message. This attack could be prevented if the message integrity check included knowledge of the WEP key as some part of its calculation.

### **Message Decryption**

This weakness results from the fact that WEP only encrypts the data as it travels over the airwaves. The message is decrypted once it has been successfully received by either a station or an AP and in the case of an AP, is then sent unencrypted over the wire connected to the AP. Thus an attacker which has access to both the wired and wireless sides of the network will be able to exploit this weakness to build a dictionary of keystreams which are associated with each of the IVs.

## **The University of Maryland Paper**

In March 2001, researchers at the University of Maryland also published a paper pointing out weaknesses in WEP as well as some of the proprietary security mechanisms used by vendors<sup>4</sup>. While the paper did get a fair amount of attention, it did not identify anything that wasn't already known by most people, including those in the IEEE.

### **Closed Network Access Control**

Closed Network access control is a feature used by several equipment vendors in order to provide an increased level of security and is not part of the 802.11 standard. In a closed network, the AP does not broadcast the SSID in its beacon and thus only those clients that have knowledge of the SSID and the location of the network can associate with the network. As the authors point out, this method would do little to deter a dedicated attacker since the SSID is broadcast in the clear by the probe request issued by a client when it requests an association to a network. An attacker only has to sniff packets waiting for a probe request where it can gain access to the SSID being used by the network.

---

<sup>4</sup> "Your 802.11 Wireless Network has no Clothes", [www.cs.umd.edu/~waa/wireless.pdf](http://www.cs.umd.edu/~waa/wireless.pdf).

## **Access Control Lists**

Access control lists (ACLs) define the list of client MAC addresses that are allowed to associate with a given AP. This is another mechanism used by several vendors but is not part of the 802.11 standard. As the authors point out, this method is also easily overcome by a dedicated hacker since the MAC address is broadcast in the clear with each frame, even when WEP is enabled. Since the MAC address is software programmable on many cards, an attacker simply needs to sniff a valid MAC address and program it into his card in order to circumvent the ACL.

## **Shared Key Authentication Flaw**

The shared key authentication mechanism built into WEP can be easily circumvented and the authors documented this weakness as part of their paper. The authentication challenge is broadcast in the clear by the AP and then later as encrypted by a keystream using a valid WEP key by the associating station. An attacker can sniff the airwaves to gather both of these responses in order to circumvent the shared key authentication. With both of these responses in hand, the attacker can determine a valid keystream which will allow association with the network by finding the exclusive-or of the two responses. This keystream can then be used by the attacker in his own association request to successfully associate with the network. As with the previous two attacks, it is important to note that even after successfully executing this attack, the attacker will only be able to associate with the network but cannot proceed any further unless the WEP key is also known.

## **The Fluher, Mantin, and Shamir Paper**

In July of 2001 a paper was published by Scott Fluher, Itzak Mantin, and Adi Shamir (FMS). In their paper the authors identified an attack that was fundamentally different in that it exploited a known weakness in the key scheduling algorithm (KSA) of the RC4 cipher. RC4 is widely used in many technologies today and is generally considered a secure cipher when used properly. However, the weakness was exposed by the way in which the WEP algorithm uses RC4.

In their paper, the authors identified the weaknesses in RC4 and then outlined an attack on WEP based on those weaknesses. The first weakness was that of the existence of a large class of weak keys in which a small part of the secret key used to seed the RC4 cipher determine a large number of the initial bits that result in the pseudo-random output of the cipher (significant correlation between RC4 input and output). The second weakness arises when part of the key used by the KSA is also exposed to the attacker (as with the IV in WEP). Using this weakness, the authors observed that when different exposed values are used in conjunction with a constant secret portion of the key, the attacker can derive the secret part with relatively little work by examining the initial part of the keystreams which are generated by the cipher. The authors identified a class of weak keys which used IVs of the form  $xxFFyy$ , where  $x$  and  $y$  are any hex value. The authors also showed that the length of time it took to execute the attack increased only linearly with the key length. Typically the length of time for any given attack increases exponentially as the length of the encryption key is increased.

A key comprised of the concatenation of a constant secret part with an attacker known dynamic portion as done in WEP leads to the RC4 weakness used in the attack outlined by FMS. The attack requires that the attacker collect a moderate number of packets encrypted with weak keys and then perform a statistical analysis on those packets in order

to determine the secret shared key. Once the secret shared key is known by the attacker, the attacker has full access to the WLAN as well as the data traveling over the WLAN.

### **Implementations of the FMS attack**

Shortly after the FMS paper was published, software tools became available on the internet which were based on the attack. Airsnort (<http://airsnort.shmoo.com>) and WEP Crack (<http://www.personaltelco.net/index.cgi/WepCrack>) both run on the Linux OS and require the use of modified WLAN card drivers to put the card in a “sniffer” mode where all packets received by the card are reported to the computer. The application then filters the list for those packets containing weak IVs and performs a statistical analysis on those packets to eventually determine the secret shared key. The current implementations of these applications require approximately 100,000 good packets (those encrypted using weak IVs) in before the secret key can be successfully derived. The time it takes to collect these packets is based on several variables, the two primary ones being the level of network traffic and the number of clients using the same secret key.

### **Weak IV filtering**

There are a number of things that can be done to address the FMS attack, but perhaps the easiest is the weak IV filter. The weak IV filter is implemented by having the transmitting MAC skip over the IVs that are known to be of the form outlined in the FMS attack. The weak IV filter is straightforward to implement and does not affect product interoperability. Ultimately, the weak IV filter is not considered a good long term solution since it doesn't address the fundamental insecurity. It is very likely that additional classes of weak keys not identified in the FMS paper exist, allowing attackers to exploit keys not filtered by a FMS targeted weak IV filter.

## **The 802.11i Robust Security Network**

In 2000, the IEEE initiated a task group, Task Group I (TGi) to develop enhanced security for the 802.11 standard. This enhancement was later labeled the Robust Security Network or RSN. As of the writing of this paper, the 802.11i standard is still in draft form and is likely 6-9 months from completion and ratification by the members of the 802.11 body. Upon its completion, the 802.11i draft will address all the weaknesses identified with WEP and address all known attacks. It will provide significantly improved security for legacy equipment as well as state-of-the-art encryption for future 802.11 WLAN products.

### **Overview**

The RSN can be viewed as consisting of three main pieces organized into two layers. On the lower level are improved encryption algorithms in the form of the Temporal Key Integrity Protocol (TKIP) and the Counter Mode with CBC-MAC Protocol (CCMP). Both of these encryption protocols provide enhanced data integrity over WEP, with TKIP being targeted at legacy equipment and CCMP being targeted at future WLAN equipment. Above TKIP and CCMP is 802.1X, a standard for port based access control developed by a different body within the IEEE 802 organization. As used in 802.11i, 802.1X provides a framework for robust user authentication and encryption key distribution, both features originally missing from the original 802.11 standard. It's important to understand that the pieces of the standard work together to form an overall security system, because taken individually, out of the context of the overall system, any single piece could be shown to have security weaknesses.

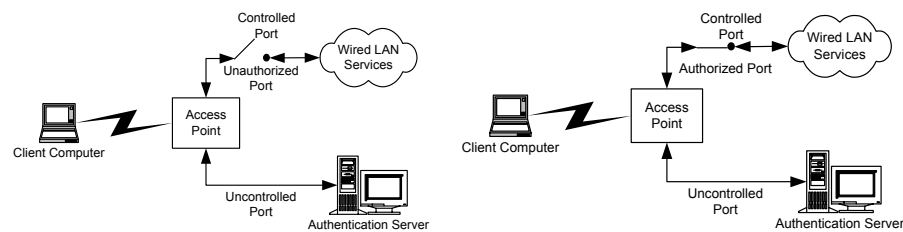
## 802.1X

IEEE 802.1X (<http://www.ieee802.org/1/pages/802.1X.html>) is a standard for port based network access control. The standard can be applied to both wired and wireless networks and provides a framework for user authentication and encryption key distribution. It can be used to restrict access to a network until the user has been authenticated by the network. It is used in conjunction with one of a number of upper layer authentication protocols (discussed later) to perform verification of credentials and generation of encryption keys.

### 802.1X in the Enterprise

There are three primary roles played by equipment in an 802.1X system. The authenticator (typically the AP in 802.11) is the port that enforces the authentication process and routes the traffic to the appropriate entities on the network. The supplicant (typically the client device in 802.11) is the port requesting access to the network. In the enterprise, the Authentication Server (AS) is a third entity that performs the actual authentication of the credentials supplied by the supplicant. The Authentication Server is typically a separate entity on the wired side of the network, but could also reside directly in the authenticator. The most common type of authentication server in use today to authorize remote users is RADIUS although other authentication services could be used. The particular authentication server to be used is not specified in the standard.

802.1X operation can be understood using the concept of a controlled port and uncontrolled port as show in 802.11 context in Figure 3 below. The controlled and uncontrolled ports are logical entities and are the same physical connection to the network. Whether a frame traveling through the AP is routed through the controlled or uncontrolled port is determined by the authentication state of the client computer. Prior to authentication by the Authentication Server the AP will only allow the client to communicate with the AS. After successful authentication by the AS, the AP will also allow the client to access other services available on the network.



• Figure 3 – 802.1X state before (left) and after (right) successful mutual authentication

The actual authentication data exchanged is a function of the upper layer authentication protocol used (discussed later) and the message protocol and routing of these messages is controlled by 802.1X. It's important to note that a mutual authentication process is used and both the network and the client are authenticated to each other. As part of the authentication process, the MAC level encryption keys used by the chosen encryption protocol will be generated. 802.1X is then used to plumb the encryption keys down to the MAC on both the AP and the client computer.

Two sets of keys are generated, session keys (also referred to as pairwise keys) and group keys (also referred to as groupwise keys). Group keys are shared amongst all the clients connected to the same AP and are used for multi-cast traffic. Session keys are

unique to each association between an individual client and the AP and create a private virtual port between a client and the AP.

802.1X enhances the enterprise security model by providing the following improvements over standard WEP:

- It provides support for a centralized security management model.
- The primary encryption keys are unique to each station so the traffic on any single key is significantly reduced.
- When used with an Authentication Server, the encryption keys are generated dynamically and don't require a network administrator for configuration or intervention by the user (this is analogous to the use of dynamic IP addresses versus static IP addresses on the network).
- It provides support for strong upper layer authentication.

### 802.1X in the Home and Small Business

In the home and small business environment most users are not expected to have a RADIUS server available for authentication. In this case, the 802.11i standard uses 802.1X in a pre-shared key configuration, however most of the previous concepts and operation remain the same. When operating with authentication server support, a master key, called the Pairwise Master Key (PMK), is generated via the exchange between the Client and the Authentication Server. The PMK is used as source material for generation of the lower level keys used by the MAC layer encryption. When no authentication server is present, the PMK is manually entered into each device in the BSS and serves as a pre-shared key for authentication and source material of the lower level encryption keys. The user model is more analogous to standard WEP in this case since it requires manual distribution and configuration of a shared secret; however this should be adequate for most small deployments.

When used in this mode, session keys are still provided and the improved encryption methods discussed below are fully supported. It's important to note that upper layer authentication is not supported and the security of the network is broken if the shared key is ever compromised. In many small deployment scenarios, these tradeoffs are likely acceptable in exchange for ease of deployment and configuration of the Wi-Fi equipment.

## **Improved Encryption**

The 802.11i standard provides two improved encryption algorithms to replace WEP. TKIP and CCMP are both called out in the standard and the standard is written in such a way that it is extensible to support the addition of new encryption protocols should they be required in the future. A BSS can support the simultaneous use of more than one encryption protocol and the client and AP will use the highest level of security that both can mutually support. However, a true RSN uses only the CCMP protocol for all equipment. A BSS which supports the simultaneous use of encryption protocols in addition to CCMP is called a transitional network and is assumed to be a temporary configuration for the purposes of converting all clients to a CCMP based security solution.

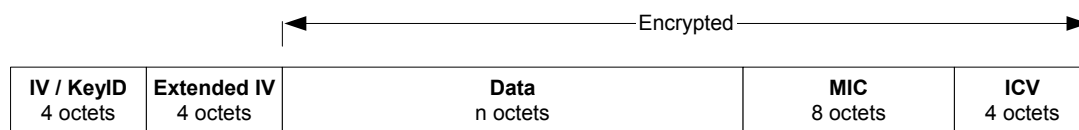
## Temporal Key Integrity Protocol

The temporal key integrity protocol was designed to address all the known attacks and deficiencies in the WEP algorithm while still maintaining backward compatibility with legacy hardware. It was designed to be made available as a firmware or software upgrade to existing hardware so that users would be able to upgrade their level of security without replacing existing equipment or purchasing new hardware.

TKIP accomplishes this by providing an additional protocol or a wrapper around WEP. TKIP is comprised of the following elements:

- A message integrity code (MIC) provides a cryptographic checksum using the source and destination MAC addresses and the MSDU plaintext data. This protects against forgery attacks.
- Countermeasures to bound the probability of successful forgery and the amount of information that an attacker can learn about a particular key.
- A 48 bit IV and an IV sequence counter to address replay attacks. MPDUs received out of order are dropped by the receiver.
- Per packet key mixing of the IV is used to break up the correlation used by weak key attacks.

The structure of a TKIP encrypted MPDU is shown in Figure 4 below. As mentioned previously, TKIP uses an extended 48-bit IV called the TKIP Sequence Counter (TSC). The use of a 48-bit TSC extends the life of the temporal key (discussed below) and eliminates the need to rekey the temporal key during a single association<sup>5</sup>. The TSC is constructed from the first and last bytes from the original WEP IV and the 4 bytes provided in the extended IV. TKIP extends the length of a WEP encrypted MPDU by 12 bytes; 4 bytes for the extended IV information and 8 bytes for the MIC.



• Figure 4 – MPDU format after TKIP encryption

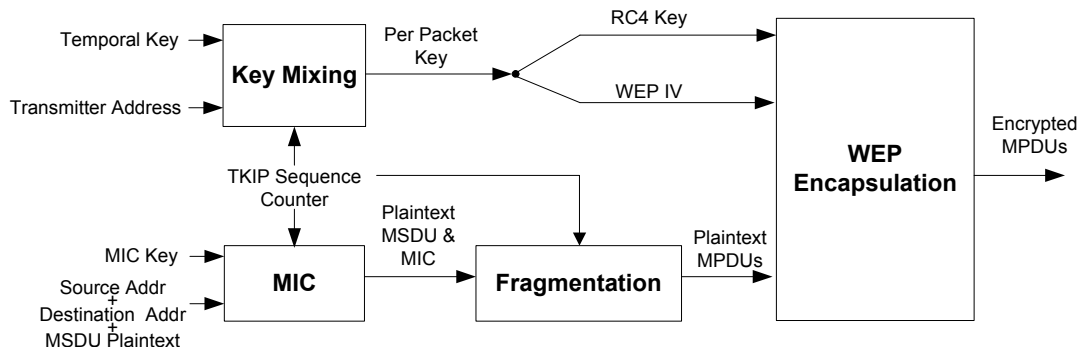
The TKIP encapsulation process is shown below in Figure 5. Temporal and MIC keys are used, which are derived from the PMK generated as part of the 802.1X exchange discussed previously. The temporal key, transmitter address, and TSC are combined in a two phase key mixing function to generate a per packet key to be used to seed the WEP engine for encryption. The per packet key is 128 bits long and is split into a 104-bit RC4 key and a 24-bit IV for presentation to the WEP engine.

The MIC is calculated by over the source and destination MAC addresses and the MSDU plaintext after being seeded by the MIC key and the TSC. By computing the MIC over the

---

<sup>5</sup> Since the TSC is updated with each packet,  $2^{48}$  packets can be exchanged using a single temporal key before key reuse would occur. Under steady, heavy traffic conditions, it would take approximately 100 years for key reuse to occur.

source and destination addresses, the packet data is keyed to the sender and receiver preventing attacks based on packet forgery. The MIC function, nicknamed Michael, is a one-way cryptographic hash function, not a simple CRC-32 as is used in computing the WEP ICV. This makes it much more difficult for an attacker to successfully intercept and alter packets in a denial of service attack. If necessary, the MSDU is fragmented into MPDUs, incrementing the TSC for each fragment, before encryption by the WEP engine.



• Figure 5 – The TKIP encapsulation process

The decapsulation process is not shown here, but is essentially the same as that shown in Figure 5 with the following exceptions. After recovery of the TSC from the received packet, the TSC is examined to ensure that the packet just received has a TSC value greater than the previously received packet. If it does not, the packet is discarded in order to prevent potential replay attacks. Also, after the MIC value has been calculated based on the received and decrypted MSDU, the calculated MIC value is compared to the received MIC value. If the MIC values do not match, the MSDU is discarded and countermeasures are then invoked. These countermeasures consist primarily of rekeying the temporal key while controlling the rate at which this happens and sending alerts to network administration for follow-up.

### Counter Mode with CBC-MAC Protocol

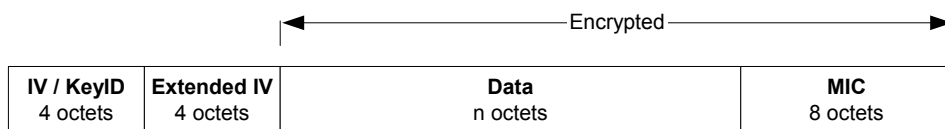
In addition to TKIP encryption, the 802.11i draft defines a new encryption method based on the Advanced Encryption Standard (AES). AES is considered state of the art in encryption technology. It has been under development for several years under funding from the National Institute of Standards and Technology (NIST) and was adopted in May 2002 by the US government as the official cipher to replace DES and Triple DES for all government transactions. Unlike TKIP, CCMP was not designed for backward compatibility and in many cases new Wi-Fi hardware which has co-processor support for AES will be required for optimal performance. In most cases, client computers with fast microprocessor support will be upgradeable to support AES with a software driver upgrade.

AES based encryption can be used in a number of different modes or algorithms. The mode that has been chosen for 802.11 is the Counter Mode with CBC-MAC (CCM). The

counter mode is the algorithm providing data privacy and the CBC-MAC (Cipher Block Chaining Message Authentication Code) provides data integrity and authentication<sup>6</sup>.

AES is a symmetric iterated block cipher meaning that the same key is used for both encryption and decryption, multiple passes are made over the data for encryption, and the clear text is encrypted in discrete fixed length blocks. The AES standard uses 128-bit blocks for encryption, and for 802.11 the encryption key length is also fixed at 128 bits. Unlike TKIP, CCMP is mandatory for anyone implementing an RSN.

The format of an AES encrypted MPDU is shown in Figure 6 below. The packet is expanded by 16 bytes over an unencrypted frame and is identical to a TKIP frame with the exception of the legacy WEP ICV included in a TKIP frame. Like TKIP, CCMP also uses a 48-bit IV called a Packet Number (PN). The packet number is used along with other information to initialize the AES cipher for both the MIC calculation and the frame encryption.

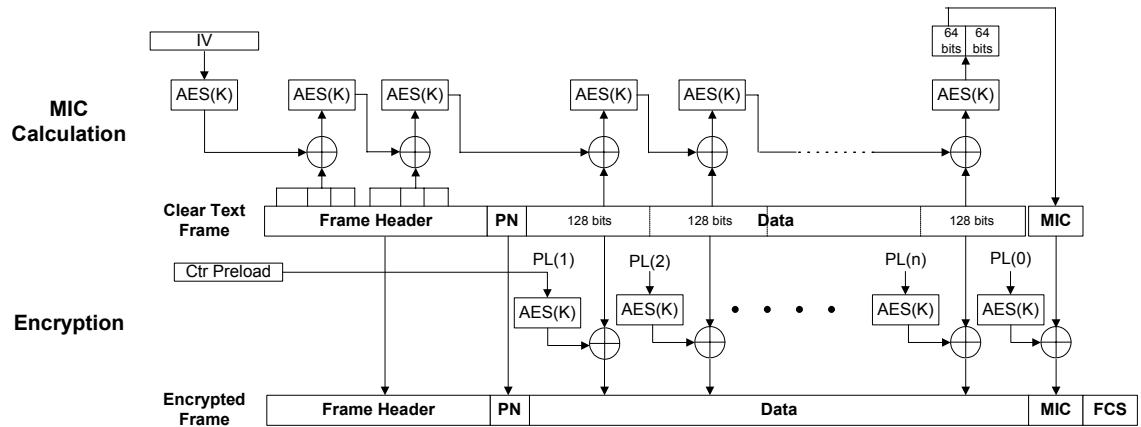


• Figure 6 – MPDU format after CCMP encryption

The CCMP encapsulation process is shown in Figure 7 below. The AES encryption blocks in both the MIC calculation and the packet encryption use the same temporal encryption key (K in Figure 7). As with TKIP, the temporal key is derived from the master key that was derived as part of the 802.1X exchange discussed previously. The MIC calculation and encryption proceed along parallel paths as shown in the figure. The MIC calculation is seeded with an IV formed by a flag value, the PN, and other data pulled from the header of the frame. This IV is fed into an AES block and its output is XORed with select elements from the frame header which is then fed into the next AES block. This process continues over the remainder of the frame header and down the length of the packet data to compute a final 128-bit CBC-MAC value. The upper 64 bits of this MAC are extracted and used in the final MIC appended to the encrypted frame.

The encryption process is seeded by a counter preload also formed from the PN, a flag value, data from the frame header, and a counter value which is initialized to 1. This preload value is fed to the AES block and its output is XORed with 128 bits of clear text from the unencrypted frame. The counter value is incremented by one and this process is repeated for the next block of 128 bits of clear text. This process continues down the length of the frame until the entire frame has been encrypted. The final counter value is set to 0 and input to an AES block whose output is XORed with the MIC value computed previously before appending to the end of the encrypted frame for transmission.

<sup>6</sup> In this case MAC is used in the cryptographic sense as Message Authentication Code and is synonymous with the term MIC used for TKIP.



• Figure 7 – The CCMP encapsulation process

The CCMP decapsulation process is not shown but is essentially the reverse of the encapsulation process of Figure 7. A final step is added to compare the value of the computed MIC to that received before the decrypted frame is passed on by the MAC.

## Authentication Protocols

Upper layer authentication (ULA) protocols are not specified in the 802.11i standard, but will be an integral part of the security system in the majority of deployments. ULA protocols were not included in the 802.11i standard because they generally operate at the transport layer of the OSI network layer model and are therefore outside the scope of the 802.11 standard.

## Overview

There are a number of popular ULA protocols in use today, primarily in the enterprise environment where the network infrastructure is in place to support their use. The ULA protocols are used to provide a mutual authentication exchange between the client and an authentication server somewhere on the network and to generate session keys to be used between the client and the AP over the wireless link. They work in conjunction with 802.1X, where 802.1X is used to enforce their use and route the messages properly, and the ULA protocols define the actual authentication exchange that takes place. In most cases a RADIUS server will be used for authentication since many companies are already using RADIUS for their dial-up users. Some of the more popular authentication protocols are discussed briefly below.

### Extensible Authentication Protocol with Transport Layer Security (EAP-TLS)

EAP-TLS is a certificate based authentication protocol and is supported natively in Windows XP. It requires initial configuration by a network administrator to establish the certificate(s) on the user's machine and the authentication server, but no user intervention is required thereafter. The certificates are digital signatures which are used in conjunction with public key encryption techniques to verify the identity of the client. During an EAP-TLS exchange, the client and authentication server exchange credentials and random data in order to simultaneously synthesize the encryption keys at both ends of the link.

Once this has been completed, the server sends the encryption keys to the AP through a secure RADIUS channel and the AP exchanges messages with the client to plumb the encryption keys down to the MAC encryption layer.

### **Protected Extensible Authentication Protocol (PEAP)**

PEAP is an IETF draft standard and can be used to provide a secure password based authentication mechanism. Although it has not been implemented in any products to date, this is likely to change in the near future. In a PEAP exchange, only the authentication server is required to have a certificate. After the initial communication with the authentication server, the public key from the AS certificate is sent to the client computer. The client computer then generates a master encryption key and encrypts this key using the AS's public key and sends the encrypted key to the AS. Now that the master key is on both ends of the channel, this key can be used as source material to establish a secure tunnel between the AS and the client over which any subsequent authentication method can be used to authenticate the client computer to the AS. In many cases it is expected that this will be some form of a password based authentication protocol.

### **Other Authentication Protocols**

Other authentication protocols worth noting include EAP-TTLS and LEAP. The Extensible Authentication Protocol with Tunneled Transport Layer Security (EAP-TTLS) is also an IETF draft standard and can be used to provide password based authentication of the client computer. EAP-TTLS is very similar in operation to PEAP and has been implemented in some RADIUS server & supplicant software designed for use in 802.11 WLAN networks.

The Lightweight Extensible Authentication Protocol (LEAP) is a proprietary standard developed by Cisco Systems and was designed to be portable across a variety of wireless platforms. It has gained popularity due to the fact that it was the first, and for a long time, the only password based authentication scheme and it also provided this support across several different client operating system platforms. LEAP is based on a straightforward challenge-password hash exchange where the authentication server issues a challenge to the client and then the client returns the password to the authentication server after first hashing it with the challenge text sent by the AS.

## **Conclusion**

The 802.11i draft standard provides a system for greatly enhanced security for users Wi-Fi equipment. Through the use of improved encryption protocols and the 802.1X standard for improved authentication, the 802.11i draft provides for a robust security solution that addresses all of the shortfalls in the current standard. It provides improved security for legacy Wi-Fi hardware as well as future Wi-Fi hardware. Work is ongoing in the standard and final ratification is expected sometime in the fall of 2003. However, since many parts of the standard are now considered firm, it is likely that the Wi-Fi industry will respond with interoperable, standards based solutions prior to formal ratification of the standard.