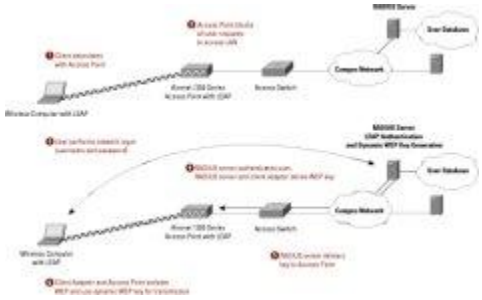
MIC (Message Integrity Check)

A message integrity check (MIC), is a security improvement for WEP encryption found on wireless networks. The check helps network administrators avoid attacks that focus on using the bit-flip technique on encrypted network data packets. Unlike the older ICV (Integrity Check Value) method, MIC is able to protect both the data payload and header of the respective network packet.

What is WEP Encryption?

Wired Equivalent Privacy (WEP) is an encryption Feature defined in the IEEE 802.11 standard. Implementation of WEP is optional, but it is designed to prevent the modification or disclosure of information contained in network data packets while they are being transported to the destination computer host. WEP is also used to help network administrators provide a layer of access control for a WiFi network and can help make a wireless network approach the security of a wired network. The WEP definition incorporates the use of the RC4 encryption algorithm using either a 104 or 40 bit encryption key. Since the same key is sued for both the encryption and decryption of data, RC4 is a symmetric algorithm. Once WEP is turned on or enabled on a wireless network, each station or computer host on the network has the key used for the network. This key is used to encrypt the data prior to sending over the air. If there is a data packet received that is not encrypted with the appropriate key, then the data packet will be discarded and never delivered to the host computer.



How Does RC4 Encryption Work?

The RC4 encryption algorithm first makes a pseudorandom stream of bits that comprise the keystream for the cipher. The stream is then used to encrypt data by combing the text with the plaintext using the XOR mathematical operation. In order to decrypt text, the reverse of the process is applied to the encrypted text. Before creating the keystream; however, the algorithm is initialized using a variable length key. For WEP encryption, this key can be either 40 or 104 bits in length. After the permutation is created by the cipher, the stream of bits is then created using PRGA (a pseudo-random generation algorithm).

How Does the RC4 KSA Work?

The key scheduling algorithm (KSA) in RC4 is used to help initialize the information stored in the array and is set to the total number of bytes stored in the key. The array will then be used to initialize the identity permutation of the cipher. The array will be used by RC4 for a total of 256 iterations and include bytes of the key at the same location during the operation of the cipher.

What are the Various Encryption Models used in WiFi Networks?

At the time of this writing, some of the most used encryption methods in WiFi networks include: AES, WEP, and TKIP. The AES method is based on hardware, but is considered to be the most secure and fast method available for network encryption. Both the TKIP and WEP encryption methods; however, are based on firmware. If not dealing with legacy firmware on a network router, a WEP capable device is able to also support TKIP and considered interoperable with each other. WEP is considered to be the weakest of the available encryption methods available for WiFi networks.

How Does Broadcast key Rotation Work?

Some WiFi network routers support the concept of Broadcast key rotation. This allows the network access point to create the best possible random group key. When the key is rotated, client computers that are capable of key management will be updated by the access point. When this feature is enabled on an access point, the router will use a dynamic broadcast WEP key and then change the key at the intervals you set in the AP. In the field, this concept is a useful alternative to implementing TKIP if the network supports dis-similar hardware that may not be able to use TKIP easily.

How Does TKIP Work?

TKIP (Temporal Key Integrity Protocol) was originally created in order to help address the natural shortcomings found with WEP encryption. The concept is also known as WEP key hashing and the original name for the method was WEP2. TKIP addresses the WEP key reuse issue (the aspect that makes the encryption method “crackable”), through the use of changing the temporal key with every data packet.

The same RC4 encryption algorithm is used, but by using the hash value to determine the temporal key, this value is different for every packet sent over the wireless network.

Do TKIP and WEP Work Together?

Technology has improved to the point over the years, that wireless networks that have existing access points that use WEP encryption are able to be upgraded to use TKIP. The upgrade requires a firmware update if legacy routers are installed on the network before the option will be available to network administrators to impalement. Equipment that is not able to be updated is still able to communicate with TKIP enabled computer hosts; however, the exchange of information will not be as secure.

What is WPA?

WPA (Wireless Protected Access) is a standards-based security solution designed to address all of the known vulnerabilities with WEP (Wired Equivalent Privacy) as defined in the original IEEE 802.11 implementation. WPA is designed to provide improved access control and enhanced data protection. WPA can be implemented at both the home office or enterprise level, and has been incorporated into most major networking hardware sold on the market.

How Does WPA2 Work?

WPA2 is the succeeding security standard by the IEEE to WPA and is defined in the 802.11i standard. This implementation adopts the AES (Advanced Encryption Standard) algorithm along with the use of CCMP (Counter Mode with Cipher block Chaining Message) . The AES Counter Mode works as a block cipher and is able to encrypt 128 bits of data (in blocks) using a 128 bit key for the encryption. WPA2 provides a much higher level of security than WPA. The model does this by creating a new session key on each association with each client key used on the network being unique to the given client. As a result, every network data packet transmitted over the network is encrypted with its own, unique key.

When comparing WPA and WPA2, each encryption method is able to use either CCMP or TKIP encryption. The fundamental difference between the two methods is with the information that is included in the 4-way handshake frames, association frames, and the beacons. WPA2 also includes the initial group key in the 4-way

handshake, and the first group key handshake is skipped. The original WPA algorithm requires this initial handshake in order to deliver the first group keys. Some people confuse the ability of WPA (original) to use AES as providing the same level of protection or security as WPA2, but this is not the case.

What is AES?

AES (Advanced Encryption Standard) is the NSA (National Security Agency) approved encryption standard. It uses the Rijndael algorithm that consists of a block cipher using a 256, 192, or 128 bit key and is considered significantly stronger than RC4. In order to support AES, the wireless network hardware and supporting computing devices must be capable of supporting AES instead of traditional WEP encryption.

How Does MIC Work?

MIC is designed to protect both the data payload and header on a WEP encrypted network. It is considered to be an enhancement to the existing WEP encryption standards and prevents network attackers from conducting bit-flip attacks on encrypted network traffic. During this type of network attack, an intruder will first intercept an encrypted message. Then, he or she will alter the message and retransmit the data packet. MIC helps prevent this type of attack by adding a MIC field to the respective wireless network frame. This feature provides an integrity check that does not have the same vulnerability to attacks that have been observed with the ICV method. Additionally, MIC adds a sequence number field to a wireless frame. If frames are received out of order by a wireless access point, then they are subsequently dropped.

What is the “Man in the Middle” Attack?

The “Man in the Middle” attack is a form of actively listening to or eavesdropping on network traffic of one or more computer hosts. In this method, the attacking computer will make an independent connection with each identified computer host or “victim.” Once establishing these connections, the computer will then relay messages between the victims creating the illusion of each computer communicating with the other via a secure connection. This dialogue; however, is fully controlled by the rogue computer or attacker. In order for the attack to be a

true “Main in the Middle” attack, 100% of the network traffic has to be controlled. The attack focuses on the lack of mutual authentication between the two victims.

How Does MIC Prevent the “Man in the Middle” Attack?

MIC (message integrity check) that is incorporated into WPA (WiFi Protected Access) is designed to include a frame counter to prevent the “Man in the Middle” attack from occurring on a WiFi network. If a MIC error is thrown, that means that the wireless frame has been rebroadcast by a third party or the client computer has a fault. If a computer client is unable to consistently pass the MIC check, the network controller will disable the wireless LAN for approximately 60 seconds per the WPA protocol. This feature helps to prevent an overall attack on the network’s encryption. The various controllers are not able to turn off the MIC errors when thrown.

Source: http://www.tech-faq.com/mic-message-integrity-check.html