Wi-Fi Security

Ryan Conrad

CSU Stanislaus

CS 4960

Dr. Melanie Martin

Introduction

The computer science field has always had a problem with data security. With increases in the profitability of data sales need for security is at an all time high. Over the years the industry has created sets of protocols for Wi-Fi usage. As time passed more and more vulnerabilities started to creep up leading to the next set of protocols. Along with sets of protocols they have started using encryption on top of using protocols. The encryption has added another layer of protection to the security of Wi-Fi networks. The game of Wi-Fi security is trying to stay one step ahead of the attackers. This paper will discuss some of the protocols and encryption methods being used for Wi-Fi security today.

Encryption is a process that converts information into an unintelligible code that someone just looking in can't read. This is commonly done by using a program to jumble up the data mathematically and send it to the caller. The caller then uses the program to undo the original jumble with the same mathematic process. This works as long as the attackers don't also know what process you are using and where to gain the knowledge of what you are using.

With Wi-Fi security you aren't just protecting yourself and your data. With a network of interconnected systems any intrusion could lead to an infection of all users on the network. This makes using the best available security a top priority for your safety and the safety of those trusting you to keep them secure.

Basic

Wi-Fi is a short-range wireless radio frequency transmission system (Peng 2012). This has to use the open air waves which anyone can listen to or broadcast on the same channel. This can lead to unauthorized access and data corruption. With the growing popularity of Wi-Fi the security of networks has been consistently growing to plug holes and prevent new holes.

Wired Equivalent Privacy

The first algorithm this paper will discuss is Wired Equivalent Privacy (WEP). This is an encryption algorithm aimed to provide secure communication between two users in a wireless local area network (WLAN). This was introduced with the IEEE 802.11-1997 standard. In its simplest form WEP is providing security with simple authorization and data encryption. WEP has two types of connection open and shared key. The open just means anyone who can grab the signal can connect to the network and begin sending and receiving data. The shared key method will be what this paper will focus on as it is the way to secure your network.

WEP uses a shared key mechanism adopting stream cipher Rivest Cipher 4(RC4) with two key sides (Sebbar 2016). RC4 uses a pseudo-random number generator to generate a bit stream from a WEP seed (Moen 2014). This stream is a concatenation of 24-bit initialization vector and 40-bit key. The key can also be comprised of a 40 bit confidentiality key and a 104 bit authentication key.

To get the ciphertext you must run an ExclusiveOR function on the generated key stream with plain text and the integrity check value (ICV) from using CRC-32. Using the ICV to protect your ciphertext against an unauthorized modification acts like a fingerprint for each message (Moen 2014). To finish off the algorithm it concatenates the encrypted ciphertext with the current initialization vector (IV) that is used to decrypt the message. This results in a complete message that can be sent over the network and decrypted by the intended receiver.

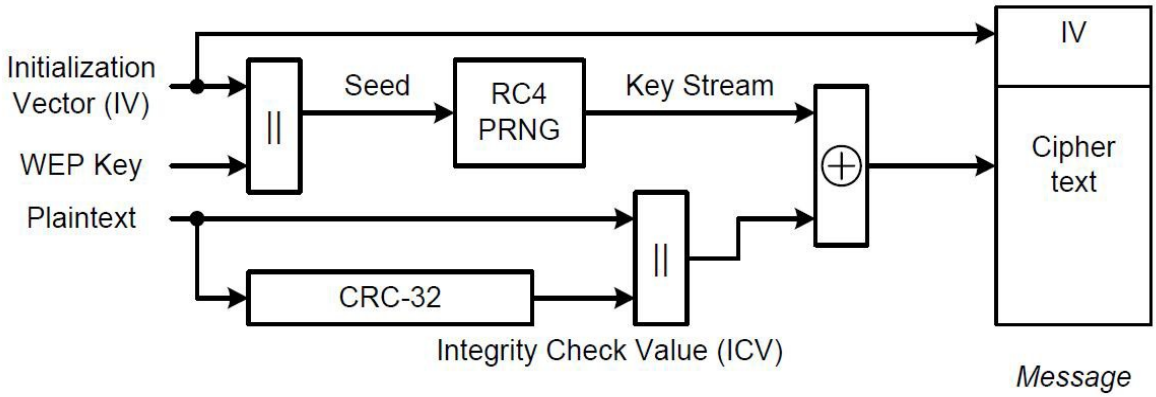


Figure 1: A block diagram of WEP encryption(802.11, 2007)

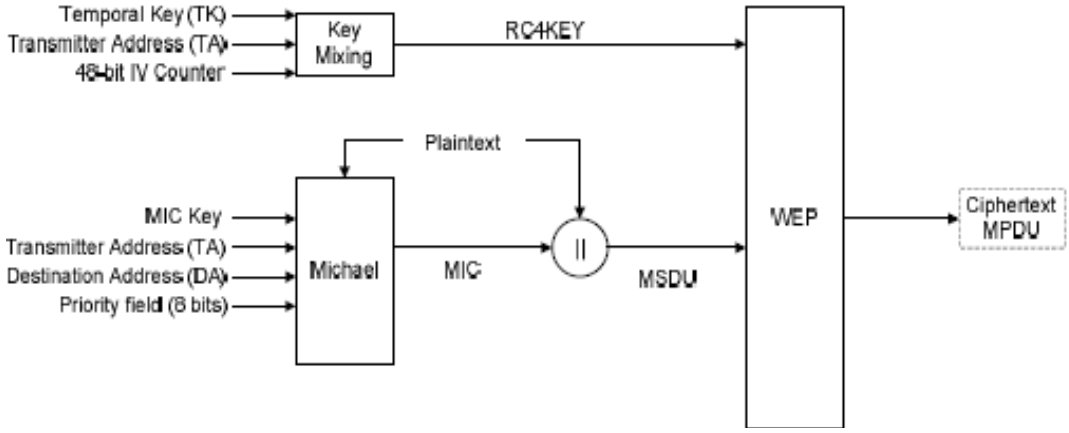
The process of decryption is done in reverse order. After the receiver gets the message it is separated from the unencrypted IV and generates the correct key stream. This process also requires that both parties in the wireless exchange know the encryption key. The receiver then decrypts the message by using the same XOR function and calculates a new ICV and compares it to the one they received from the sender to validate the integrity of the data (Moen 2004).

In today's technological age WEP is mostly an obsolete protocol as it does not provide an acceptable level of security. In many of the shared key implementations of a WEP network the same key is used through the network leading to a non-unique authentication. Since the same

keys are used throughout every malicious attack that gains access to the key can connect to the network. The keys are manually distributed and can become problematic with a larger user base (Peng 2012). In addition, the CRC-32 algorithm which generates the ICVs is cryptographically insecure because it is linear. The algorithm produces a similar signature for similar messages without using any initialization values making it possible to modify data without breaking the checksum run at the end(Moen 2004).

Wi-Fi Protected Access

Another algorithm in use is Wi-Fi Protected Access (WPA). WPA was an improvement over the WEP security. It employs the Temporal Key Integrity Protocol (TKIP) rather than the RC4 that WEP uses. This was not the only change as WPA also used a stronger integrity checking algorithm called Message Integrity Code (MIC) to replace the CRC32 of WEP.



Firgure 2 TKIP encryption diagram

WPA security uses a 128-bit Temporal Key. This key is obtained during the authentication/key distribution process. The TK is used with transmitter address and IV in the key mixing function. After this hash function you will receive a unique 128-bit frame key (WEP or RC4 key). This ensures that the secret key is not used directly in the encryption process (Housley 2002). TKIP also uses a TKIP Sequence Counter (TSC), which makes sure that the frame-key is only used for one frame. The counter increases after each packet acting as a defense mechanism against data reply attacks as the receiver will ignore packets with incorrect TSC. TKIP provides better data integrity with the Message Integrity Code (MIC) created from the Michael algorithm (Ferguson 2002). The algorithm takes in many inputs; 64-bit MIC, Destination address, Source address, Priority field, and unencrypted plaintext.

The TKIP encrypts the MIC to make forging MIC harder on an attacker. After being calculated the MIC is concatenated with the plaintext and forwarded to encryption. The encapsulated WPA frame is then sent to the receiver(802.11, 2006).

Decapsulation of the WEP frame is started by checking that the TSC is correct. The message will be deleted if the TSC is incorrect. If everything is in order the ciphered Medium Access Control Protocol Data Unit(MPDU) is sent to the WEP decapsulation process(802.11, 2006). The Frame Check Sequence(FCS) and ICV are checked before calculating the MIC. Before decapsulation can occur a WEP seed must be created. The receiver and sender calculate frame keys in similar fashion and give the seed to WEP as an IV. If WEP decapsulation is successful, the defragmented Medium Access Control Service Data Unit(MSDU) is sent to the next step of decapsulation. If this process failed the packet will be discarded. After the

defragmentation process TKIP checks for a valid MIC in the packet.

The WPA protocol managed to fix the main problems with the WEP process by providing enhanced encryption and key authentication. This was only temporary as they used an older cyptographic algorithm. Using a hash function inside the TKIP key mixing function can also produce unintended threats like hash collisions(Sarmi, 2008).

Wi-Fi Protected Access Version 2

As with most good software when there's a good base you just need to improve upon it and make another more secure version. This is what was done with the production of WPA2. WPA2 was also known as IEEE 802.11i-2004 (Sebbar, 2016). With this new version they introduced Counter Mode CBC-MAC Protocol (CCMP) which was a new Advanced Encryption Standard (AES) encryption mode that was better than TKIP. Version 2 still uses the same message integrity and authorization as WPA.

The AES system used a symmetric-key algorithm that used a 128 bit key for both encrypting and decrypting your data. In the WPA2 implementation of AES the message is encrypted in 128-bit blocks that are calculated independently. TKIP is also supported in WPA2 to help with backward compatibility issues with older hardware.

With the usage of CBC-MAC mode ensure data integrity by generating a chained authentication component from an unencrypted frame. This is an improvement on the Michael

algorithm was used for the MIC generation. This also removes the threats from hash-functions in the TKIP key mixing function (Sarmi, 2014). The algorithm consists of the following steps:

1. Creation of an initialization block
    - 8-bit Flag field that is set to 01011001
    - 8-bit Priority field set to 0
    - 48-bit Transmitter Address
    - 48-bit Packet Number
    - 16-bit Data Length field

Bit index	0-7	8-15	16-63	64-111	112-127
Content	01011001	00000000	Transmitter address	Packet number	Data length

2. XOR function is used on the result from step one and selected 128 bits from the 802.11 frame header: Frame Control, Address 1, Address 2 and Hlen.
3. The result from step 2 is introduced into AES
4. XOR function is used on the results of step 3 and selects fields from the frame header: Address 3, Sequence Control, Address 4 and Quality of Service Control.
5. Step 4 results are ciphered with AES
6. XOR function is applied to the result from step 5 and the first 128 bits of the payload
7. Step 6 results are ciphered with AES to prduce a 128-bit block.
8. Steps 6 and 7 are repeated until the entire payload has been ciphered.

If the final block is less than 16 octets (128 bits) it is padded with zeroes to match in size. These steps produce the results of a CBC-MAC algorithm in a 128-bit block that was generated over the whole frame, starting from the headers to the end of the payload, in a chained manner. The 64 most significant bits are taken the represent the MIC for this frame and concatenated

unencrypted to the end of the payload before ciphering with the AES counter mode.

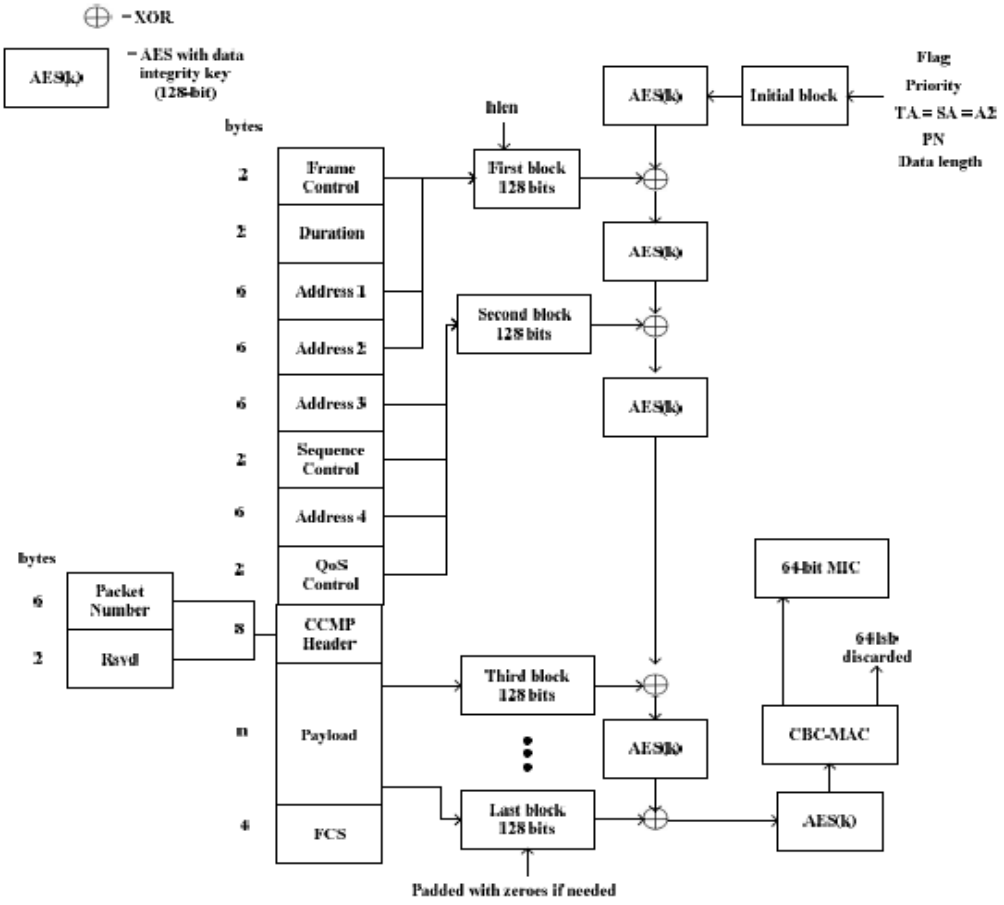


Figure 3 CBC-MAC Algorithm

The counter mode algorithm encrypts data and the MIC in the following steps:

1. An initial block is constructed from the following components:
    - 8-bit Flag field that is set to 01011001
    - 8-bit Priority field set to 0
    - 48-bit Transmitter Address
    - 48-bit Packet Number
    - 16-bit Counter which is fixed at 1 and increased for every 128-bit block until everything has been encrypted
      The constructed IV block is ciphered with AES and data encryption key.

The constructed IV block is ciphered with AES and data encryption key.

Bit index	0-7	8-15	16-63	64-111	112-127
Content	01011001	00000000	Transmitter address	Packet number	Counter

2. XOR function is applied to these results and the first 128-bits of the clear text payload. This will produce the first 128 ciphered bits.
3. The counter from the IV is increased, ciphered with AES, and XORed with the next 128 bits of the payload. This step will be repeated until the payload and concatenated MIC has been encrypted. For MIC encryption the counter of the initial block is not increased, but instead set to 0. Only the 64 most significant bits are XORed with the MIC.

The following figure shows the functionality of AES in counter mode for the 802.11 standard. The decapsulation of the encrypted MPDU is done in reverse order. If the PN is invalid the packet will be deleted. The MIC calculated in the receiver side must also match the one created during the encryption within the frame.

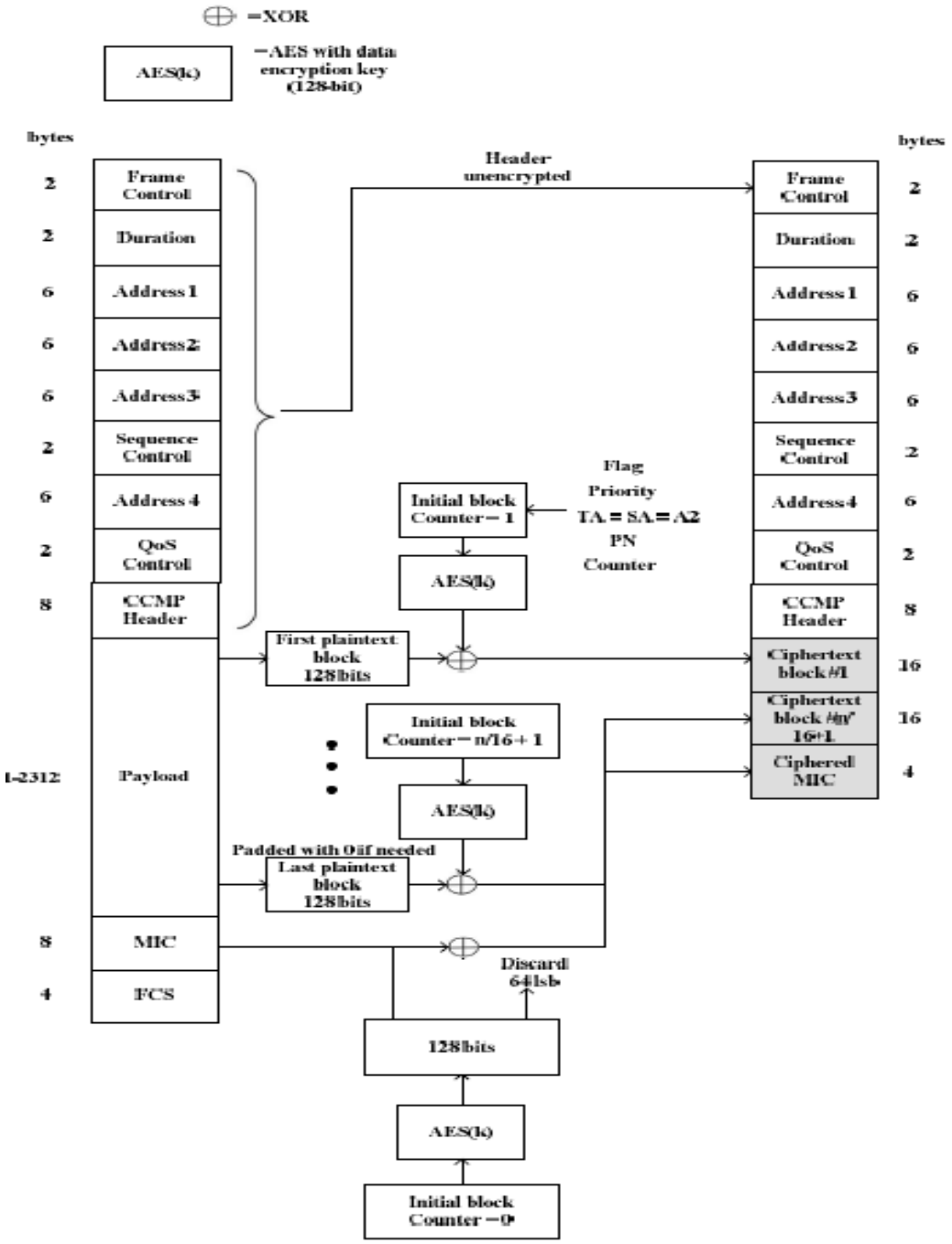


Figure 4 AES in Counter Mode

Conclusion

With the invention of Wi-Fi came the need for better security for data protection. With this need in the open groups began looking for protocols and algorithms to lock unauthorized users out. This led to the creation of Wired Equivalent Privacy or WEP. The insecurities in WEP led to the creation of Wi-Fi Protected Access or WPA. While WPA improved upon the WEP it was developed in haste and used inferior techniques to produce a minor improvement. The newest Wi-Fi security is WPA2 which started using a better encryption method while still being able to maintain backward compatibility with older hardware.

Even with these advancements no Wi-Fi network is completely safe. The fight for security is a never ending battle. Most of these security sets are just stopping the easy hacks from allowing everyone to steal data. Every algorithm eventually becomes known and broken allowing hackers to gain access to systems and data. With the current security end users can more than likely expect home networks to remain secure. However with public Wi-Fi networks users can never expect to have real security. There is not only the potential for random listeners to steal info or install malware on the users system, the owners of the networks often times want access to users information.

References

Niels Ferguson, “Michael: an improved MIC for 802.11 WEP”, IEEE document 802.11-02/020r0, 2002, Web. November 2017.

V. Moen, H. Raddum, and K. Hole, “Weaknesses in the temporal key hash of WPA”, *ACM SIGMOBILE Mobile Computing and Communications Review*, pp. 76-83, April 2004, Web. November 2017.

IEEE Std. 802.11i -2004, “Medium Access Control (MAC) Security Enhancements”, IEEE Computer Society, June 2004, Web. November 2017.

IEEE Std. 802.11 -2007, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, IEEE Computer Society, June 2007, Web. November 2017.

O. Sarmiento, F. Guerrero, and D. Argote, “Basic Security Measures For IEEE 802.11 Wireless Networks”, Ingenieria e investigacio, pp. 89-96, vol. 28, issue 002, 2008, Web. November 2017.

A. Sebbar, SE. Boulahya, G. Mezzour, M. Boulmalf , “An Empirical Study of Wi-Fi Security and Performance in Morocco -WarDriving in Rabat”, 2nd International Conference on Electrical and Information Technologies ICEIT’2016, Web. November 2017.

R. Housley, D. Whiting, and N. Ferguson, “Alternate temporal key hash”,

IEEE document 802.11-02/282r8, April 2002, Web. November 2017.

H. Peng, “Wi-Fi network information security analysis research”,IEEE Computer Society, 2012, Web. November 2017.