Wireless Network Security

Liam Kiemele V00154530

March 5, 2011

Wireless networking is becoming increasingly prevalent in modern networked environments. This paper examined methods used to secure wireless networks from intrusion and eavesdropping. WEP, WPA and RSN were examined to see the progression from weak to much stronger security for wireless LANs. WEP was incredibly insecure, but these vulnerabilities were addressed to produce significantly more secure networks.

1 Introduction

Wireless networks are significantly different from wired networks. In order to obtain access to a secured wired network one must either have a physical connection inside the network, or traverse the network firewall. Essential a user or attacker must either be on-sight, granted access or bypass a firewall. With wireless networking it may be possible to circumvent these protections.

1.1 Security Motivation

There are several major reasons to have security measures in place for wireless networking. Without protection, they are significantly less secure than wired networks. Like most security applications, wireless security seeks to address both the confidentiality and integrity of data. This involves securing data from eaves dropping and more active attacks, such as forgery. Traditionally, availability has been less of an issue, but denial of service attacks on wireless networks are starting to appear.

In order to send and receive packets on a wireless network, one only has to be in radio range. This has serious security implications. Eavesdropping can be particularly easy to perform and is more or less undetectable. An attacker does not even have to connect to the network; they can use promiscuous mode on their network card to eavesdrop on any unprotected packets.

This poses problems because internal resources may only be protected from outside networks and not internally. A good example is an internal website. It may contain confidential information and be protected from external attacks by a firewall. The assumption is it will not be attacked internally. If an attacker can gain access to the wireless network, they may be able to obtain access to confidential services.

Another serious threat is eavesdropping. Modern switched Ethernet generally does not have this problem as packets will only travel to their proper destinations. Wireless connections on the other hand are forced to broadcast packets and these can be picked up by anyone with a capable wireless card. Essentially the tools required for attacking a wireless network are a laptop and wireless card capable of entering

promiscuous mode. Both are easily obtained.

1.2 Security Technologies

This report examines three standards used to secure wireless networking: Wired Equivalent Privacy, Wi-Fi Protected Access and RSN. The each address the issues of confidentiality and integrity with varying degrees of success. This report will discuss both the methods of protecting data, their vulnerabilities and how these vulnerabilities were mitigated in the following standards. The progression from WEP to WPA and then RSN shows how standards can be improved and also how new vulnerabilities may appear.

2 WEP

2.1 background

WEP was created to allow for the equivalent privacy and security as with a wired connection. This was one of the first security standard used to protect wireless communication. It was created with three goals in mind: to prevent eavesdropping, to protect access and to ensure data integrity. For this reason, it supports authentication, encryption and an integrity check. To encrypt and decrypt, WEP single 40 or 104 bit key. The system in total can support four different keys in use. WEP is now depreciated as it did prove to be secure. [7]

2.2 Security Measures

2.2.1 Authentication

WEP supports two type of authentication.

Open System Authentication allows any client to request access and authenticate with the wireless access point. The authentication itself does not require any shared keys, though communication may be encrypted with a WEP key. In essence Open System Authentication authenticates any client which can communicate with the access point.

Shared Key authentication relies on the client and access point using a shared key to authentication. This uses a four way handshake [8].

1. The client requests authentication
2. Access point responds with a plaintext challenge
3. Client then encrypts the challenge text in a WEP frame and responds to the access point.
4. The access point can then decrypt the frame and check to see if it has received the correct response. It then responds with accordingly.

2.2.2 Confidentiality and Integrity

WEP uses fairly simple process to encrypt encapsulate packets. This can be seen in figure 1. || represents a concatenation and $\oplus$ represents an xor operation. Figure 2 shows encapsulated packet. It includes and Initialization Vector, the data the ICV integrity checksum.

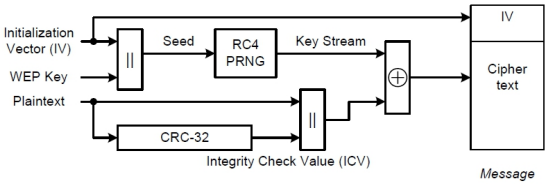


Figure 1: WEP Encryption [7]

To ensure confidentiality, WEP frames are encrypted using the RC4 stream cipher.

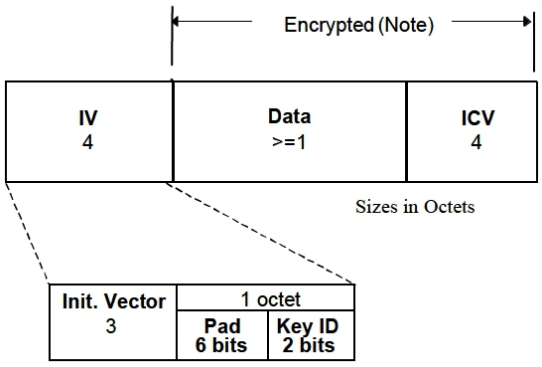


Figure 2: WEP Encryption [7]

This uses either a 40 bit or 104 bit key and a 24 bit initialization vector. The initialization vector is sent as plaintext with the packet and is concatenated onto the key to form the RC4 seed. With a 40 bit key this becomes 64 bits and with a 104 bit key this becomes 128 bits.

To ensure message integrity the CRC-32 of the transmitted data is calculated and appended to the frame. This is also encrypted with the RC4 stream cipher.

Decryption of a packet is essentially the same process in reverse and can be seen in figure 3. If the integrity check fails, the packet will be discarded and an error message is generated.

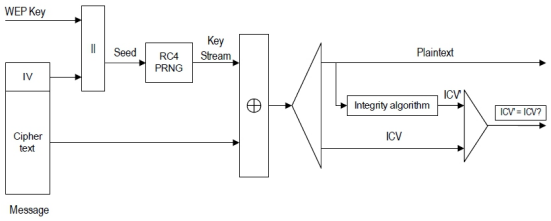


Figure 3: WEP Decryption [7]

2.3 Vulnerabilities

There are glaring flaws present in WEP which have rendered it susceptible to many attacks.

2.3.1 Keystream Reuse

The initialization vector for the RC4 algorithm is relatively short and in practice, the shared key will be changed infrequently - especially as WEP provides no method for key distribution. Initialization vectors will eventually be repeated and this will lead to the same RC4 keystreams being used to encrypt multiple messages. Also because the IV is transmitted in plaintext, an attacker will know which packets are encrypted with which key streams. Reusing the keystream is dangerous as an attacker can xor two packets together.

With two packets using the same keystream: $C = P \oplus K$ and $C' = P' \oplus K$

We can xor them to obtain :
$C \oplus C' = P' \oplus P \oplus K \oplus K$

Which becomes: $C \oplus C' = P' \oplus P$

Essentially if an attacker knows the contents of one packet they can easily learn the contents of another. Because network communication can be somewhat predictable and redundant, predictable packets can be used to decrypt others. A good example of a predictable packet is an ARP request or response - which occur fairly frequently. As packets are decrypted, the keystream for each IV can be deduced.

IV collisions are likely occur within 5000 packets - which is only a few minutes of transmissions. If one plaintext is known, an attacker can then use it decrypt other plaintext. Because communication is often

predictable, an attacker can take advantage of this to recover the plaintexts. [4]

It is also possible for an attacker to then recover the keystreams. This leads to more advanced attacks. Fluhrer, Mantin and Shamir published the FMS attack in 2001. This used two facts about wep encryption. The first is that the IV becomes the first 3 bytes of the key. The second is there is a correlation between the RC4 key and it's generated keystream. If an attacker collects enough packets, they can use this then deduce the key. This required approximately 4,000,000 to 6,000,000 packets to have a 50% success rate.

This was expanded into the KoreK attack in 2004 by adding an addition 16 correlations to the original one used by Fluhrer, Mantin and Shamir. This lowered the required packets to 700,000 for a 50% success rate.

Keystream attacks on WEP encryption have continued to improve and current attacks only require 35,000 to 40,000 packets - an amount with can be gathered in less than 60 seconds. [14]

2.3.2 Weak Authentication

WEP authentication is essentially nonexistent. Open System Authentication does not provide any authentication and shared key authentication is easily bypassed. This is because the challenge is sent in plaintext and the response to the challenge is just the properly encrypted plaintext. An attacker can XOR the challenge with the response to obtain the keystream. [1] The operation is fairly simple and shown below.

$$\text{Challenge} = P$$
$$\text{Response} = P \oplus K$$
$$\text{Challenge} \oplus \text{Response} = P \oplus P \oplus K$$
$$\text{Challenge} \oplus \text{Response} = \text{K}$$

The attacker can recover the valid keystream. It can then be used to correctly respond to any future challenges and correctly authenticate to the system.

This is one way an attacker can easily obtain a valid keystream and it can aid them in key recovery attacks. In effect, shared key authentication is less secure than Open System Authentication.

Finally, this system only supports shared keys. This is impractical for large organizations. In the case of one key being comprised, every wireless client would need to receive new shared keys. This creates serious logistical and security problems.

2.3.3 Non Cryptographic Integrity Check

The CRC-32 is not a keyed or cryptographic checksum and is easily computed. It was designed for error detection not security. An attacker who possesses a valid keystream can create arbitrary messages, compute the checksum and encrypt it using the keystream. Because WEP allows for the reuse of initialization vectors, an attacker can create any amount of arbitrary traffic.

The weak checksum is taken advantage of in the Chop-Chop attack - also developed by KoreK. The chop-chop attack allows an attacker to decrypt the last m bytes of a packet by sending $m \times 128$ packets on average.

This is done by removing the last byte of the encrypted packet and then guessing the change in the checksum. A packet is then sent with the missing byte and guessed checksum. Packets with incorrect checksums will be discarded silently and packets with correct checksums, but from unauthorized or unassociated clients will generate

error messages. If an error is detected, the change in the checksum will be the value of the last packet. [2] This is fairly similar to a padding oracle attack, but instead of attacking weak padding, it attacks a weak checksum.

3 WPA with TKIP

3.1 Background

WEP failed to accomplish its security goals and is vulnerable to several attacks. Wi-Fi Protected Access was designed to improve security by addressing vulnerabilities in WEP. For this reason the Temporal Key Integrity Protocol was constructed. It was initially used as a quick replacement to address the flaws in WEP while using existing hardware. Because of this, TKIP is more or less built on top of WEP and uses the RC4 cipher encryption. It has several security features which attempt to address the flaws in WEP. Unfortunately, because it is based on the same hardware, some of the vulnerabilities are still present.

3.2 Security Measures

TKIP adds a key exchange protocol combined with cryptographic key mixing protocol to avoid keystream reuse. TKIP also uses sequence counters to avoid replay attacks and an improved integrity check.

3.2.1 Authentication

WPA uses shared key authentication and also supports 802.1X authentication. The pre-shared key is designed for use in small business or home applications. The pre-shared key is not used to encrypt a simple challenge response. An attacker can no longer eavesdrop on an authentication and gain all the required information to authenticate with the base station. The process for authentication is tied closely with the key exchange protocol detailed further on. The support for 802.1X allows for large corporations to more easily use the standard. This allows the wireless access point to run in conjunction with other authentication technologies such as Kerberos. [3]

3.2.2 Key Exchange Protocols

The main problem with WEP was that duplicate keystreams allowed an attacker to easily exploit the system and even recover the encryption key. In order to prevent this, the TKIP algorithm not only uses several keys for communication, but these keys change in order to avoid duplication. The increased security with WPA comes from the fact no keystream is reused.

This is accomplished by using temporal keys which are changed periodically, in effect there is a hierarchy of keys. The main key is either the shared key when using pre-shared keys or a master session key obtain from authenticating with 802.1X. Either way, from this key the Pairwise Master Key (PMK) is derived. From this key a Pairwise Temporal Key (PTK) is derived using a four way handshake. The client and server both exchange nonce values. The nonce values, the access point's mac address and clients mac address are concatenated with the PMK. This value is then put through a cryptographic hash function and becomes the PTK. From the PTK, the key confirmation key, the key encryption key and the temporal key are derived. [9]

The temporal key is used to communicate with the access point. Each session has it's own unique temporal key. The key confirmation key and the key encryption key are generated to protect key man-

agement frames. The confirmation key is used in cryptographic hash functions for message integrity and the key encryption key is used to encrypt the key management frames. They are used to transmit keys securely and are not used for transmitting regular data. This allows for keys to be securely updated as required.

In order to facilitate broadcast traffic, the access point also generates a group master key (GMK). This is used for to generate a group transient key every time a client connects or disconnects. This new GTK is delivered to all clients. The GTK is then used to encrypt and decrypt broadcast or multicaste traffic. [3]

3.2.3 Confidentiality and Integrity

TKIP was designed to replace WEP without replacing the underlying hardware. This means it is still reliant on the RC4 cipher for encryption and decryption. There are several security features incorporated to address deficiencies in WEP. The encryption and encapsulation process actually involves WEP encapsulation and this is shown in figure 4.

The WEP integrity check was only a CRC-32 checksum. This has been replaced by keyed hash function which becomes the Message Integrity Code(MIC). This is verified after decryption. Unfortunately the MIC cannot provide strong protection against active attacks. For this reason, MIC verification failures are considered to be a sign of an attack. In the event of two MIC failures in less than 60 seconds, all packets are discarded for the next 60 seconds and the temporal keys are renegotiated. Halting communication for 60 seconds is done in an attempt slow down any attacks.

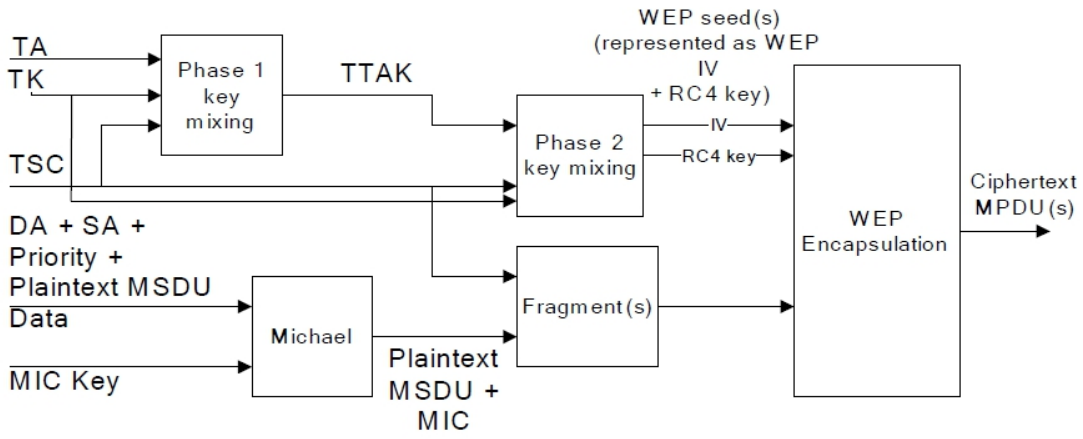
The TKIP sequence counter was implemented to prevent replay attacks. Packets received out of order will be discarded. Finally as oppose to concatenating the RC4 initialization vector with the key, TKIP uses a cryptographic mixing function. This ensures that keystreams will not be reused and prevents most attacks which were possible under WEP.

3.2.4 Key Mixing Protocol

To avoid keystream reuse, TKIP using a cryptographic key mixing protocol. This takes as inputs the transmitting address, the sequence number and the temporal key and involves two phases. The sequence counter is a 48 bit counter which is incremented for each packet. This is shown in figure 4 along with the TKIP encryption and encapsulation.

Phase 1 takes as input the temporal key, transmitting address and sequence counter and outputs 80 bits as 5 16 bit values. It is worth noting that phase 1 only uses the first 4 bytes of the sequence counter. Because it only uses the first 4 bytes, the outputs can be cached and used for the next 2^{16} encryptions. Phase 2 to takes this intermediate value along with the temporal key and sequence counter and outputs the 128 bit WEP seed. Both phases involve non-linear substitutions using an S-box. S-Boxes provide a defense against differential and linear cryptanalysis.

Key mixing allows for the combination of the 48 bit sequence counter, 128 bit temporal key and transmitting address to create a 128 bit RC4 seed. This is a significant improvement over the previous 24 bit initialization vector and helps ensure a keystream is not reused. In the event the sequence counter will repeat, new keys will be negotiated ensuring no keystream is repeated.



DA - Destination Address, SA - Source Address, TSC - TKIP sequence counter, TA - transmitting address, TK - temporal key, TTAK - intermediate key

Figure 4: TKIP Encapsulation [8]

3.3 Vulnerabilities

Because the TKIP encryption is built to be compatible with WEP hardware, it is still vulnerable to an attack which previously worked on WEP. Even though it is not vulnerable to keystream recovery attacks, it is still vulnerable to a modified version of the chop-chop attack.

The Beck Tews Attack is a modified chop chop attack which can decrypt packets on WPA. In theory, the sequence numbers and the MIC checks help prevent chop chop attacks. Unfortunately there is a quality of service feature in the WPA standard which makes it vulnerable. This feature allows for multiple transmission channels and each channel has it's own sequence counter. This means packets can be transmitted multiple times, but they must be sent on different channels. In practice, a typical network will only transmit on one channel and this leaves the rest available for an attack.

Using the modified chop chop attack, an attacker can decrypt a packet and recover the plaintext and keysteam. Then they can reverse the MIC algorithm to find the key used to calculate the MIC value. With this information an attacker can now forge packets and can transmit them on any channel where the counter is lower than value of the decrypted packet. Using the modified chop chop attack, it should be possible to forge approximately 7 packets [2]

This attack was also expanded upon by another group of researchers. They combined this with a man-in-the-middle attack. Essentially they used another computer to relay traffic from a client to a wireless access point. This allows for the attacker to control the traffic and significantly reduce the attack time. Once again, targeting arp packets can reduce the attack time to approximately one minute [14]

It is also worth noting, as a counter measure against such active attacks, two failed MIC verifications will cause transmissions to stop for 60 seconds and the temporal keys will be negotiated. This can be used

by an attacker to create a denial of service attack.

4 RSN

4.1 background

Because of the vulnerabilities in the TKIP protocol, there was a need to provide another encryption mechanism. This led to the use of the CCMP Protocol in RSN networks. The RSN standard was introduced in 2004 and incorporated in the 802.11-2007 standard. This fixes the problems present in TKIP encryption. As it no longer has to rely on WEP hardware it doesn't have any of the underlying vulnerabilities. AES and CCMP were an optional part of WPA, but they are mandatory for RSN compliance.

4.2 Security Measures

In order to address the vulnerabilities in TKIP and WEP, RSN uses CCMP which is the Counter Mode with Cipher Block Chaining Message Authentication Protocol. This addresses both confidentiality and integrity. Previously the TKIP MIC check was vulnerable to attack and the RC4 encrypted stream could be deciphered using the chop-chop attack. Because this method of encryption is completely different from both TKIP and WEP, it is not vulnerable to the same attacks. [5]

A significant advantage of using CCMP protocol is that is uses CCM mode of the AES block cipher. The CCM mode is considered to be an authentication-encryption mode. CCM both encrypts a message and produces a message authentication code using the same key. This has been proven to be a secure method of using one key to encrypt the message and generate a MAC. [11]

The AES block cipher has some desirable properties for this application. Previously predictable ARP packets were exploited to obtain keystreams. This is not possible with AES. Not only is it not a stream cipher, but it also exhibits a strong avalanche effect. This means a single change in one bit could greatly change the entirety of the ciphertext or MAC. When messages may be very similar, this is a beneficial feature.

4.2.1 Authentication and Key Exchange

Authentication is handled with the same mechanisms as WPA. This also allows for a pre-shared key or 802.11x authentication. RSN also uses the same 4-way handshake to establish the various required keys.

4.2.2 Confidentiality

Confidentiality is assured by the CCM mode of the AES Block cipher. CCM requires a 128 bit key and operates on 128 bit blocks. It also requires a unique nonce for each packet encrypted. This is obtained by combining several values. The first is a unique packet number. This should not be reused with the same temporal key. The packet number is combined with the address of the sender and the priority to form the CCM nonce. This can then encrypt the message using the AES block cipher in counter mode. [10]

4.2.3 Message Integrity and Authentication

To ensure message integrity is maintained, the CBC-MAC of the message combined with some protected header fields is calculated. This done is done by simply by taking the last encrypted block of the CBC

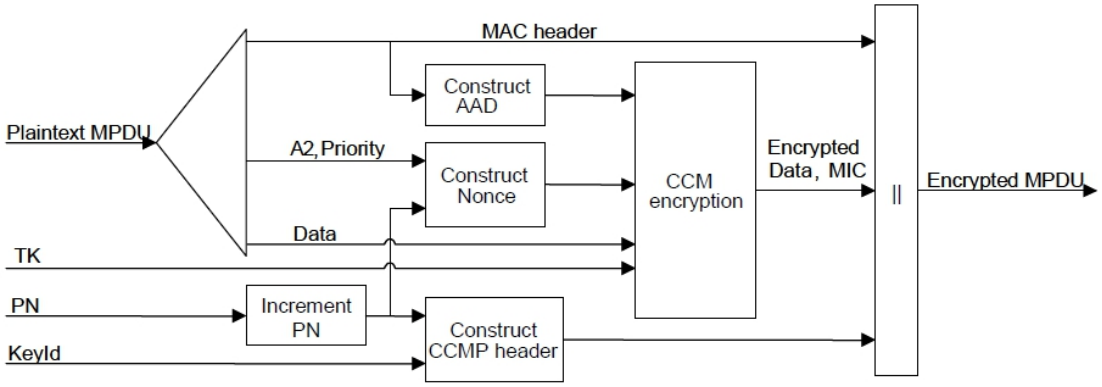


Figure 5: CCMP Encapsulation [10]

encryption. Since the chained block cipher mode depends on all previous blocks, any change in the transmitted data will cause the check to fail when decrypted. In this case the CBC algorithm works as a keyed hash function and ensures the message integrity. It also ensures that the message comes from someone who possesses the temporal key.

In addition, to protect against replay attacks, each access point and client will maintain separate sequence counters for each connection and discard any packets which are received out of order. This done done using the packet numbers.

4.2.4 Denial of Service

Previously the security mechanisms in the RSN standard were primarily concerned with confidentiality and integrity. This originally led to vulnerabilities to Denial of Service attacks. These took advantage of certain unprotected management frames to repeatedly send Deathentication or Disassociation frames. This would disrupt service as clients would be disconnected from access points. [6] The 802.11w-2009 amendment to the Wi-Fi standard prevents these attacks by protecting management frames. This is a relatively new amendment, so this may not be incorporated in legacy systems.

4.3 Vulnerabilities

RSN uses CCMP to address previously vulnerabilities in Wi-Fi security. As such it has eliminated the vulnerabilities that were exploited in both WEP and TKIP.

The problems with WEP were based around an extremely weak authentication, keystream reuse and a weak integrity value. As such it could be exploited in several ways. Packets could be decrypted and the key could be recovered. This was fixed by the changing keys regularly, improving the integrity check and adding a more robust authentication and four way handshake. The chop-chop attack that remained with TKIP has been mitigated by the face that CBC-MAC is a cryptographically secure message integrity code that cannot be reversed to recover the key.

There is a vulnerability in the current CCMP protocol. It does not exploit any weakness in AES itelf, and instead has to do with the unique nonce used with the AES cipher to encrypt the message. Be-

cause the nonce is made from the packet number, the address of the sender the priority, it may be possible for an attacker to successfully predict the nonce value. With the nonce value, it is possible to carry out the TMTO attack. This is a shortcut over a brute force attack on the temporal key which effectively reduces the search by 1/3. [12] This makes the key approximately as strong as an 85 bit key and this may be crackable by an organization with significant computing power.

More recently a vulnerability was discovered with the Groupwise Transient Keys used in both WPA and the RSN standards. This was discovered by Md Sohail Ahmad and is termed Hole 196. When using PTKs it is possible to detect forgery or spoofing. Unfortunately GTK do not allow for this detection. Therefore if an attacker possesses the GTK they can perform forgery attacks and create broadcast packets. Using approximately 10 line of code, Ahmad managed to obtain the MAC address of the access point and from their could forge broadcast attacks. With this they can be a variety of attacks. Using ARP packets they can reroute traffic to themselves and use a man in the middle attack to obtain data. This attack can only be done by someone with a GTK and this mostly limits it to authenticate users. [15] That being said, internal attacks can be common in large companies.

It is possible to brute force the shared key in psk systems using a dictionary attack, but this can be mitigated by having a sufficiently complex key or using 802.1X authentication. As of writing, there is currently a dictionary attack service which uses cloud computing to attempt to crack the key. This can try 185 million words in approximately 20 minutes. RSN dictionary attacks are now available as a service. [13] A properly chosen key should avoid this.

5 Conclusions

Wireless security is at the very least not straightforward and it took several attempts to reach our current level of security.

WEP is more or less entirely insecure as an attacker can gain access to the network in a very short period of time without requiring any special equipment. Keystream reuse, a weak integrity check and weak authentication made it extremely vulnerable. As such it was depreciated and replaced with WPA.

WPA provides the TKIP protocol which removes the problem of keystream reuse via temporal keys, but it was still susceptible to the chop chop attack because of a non-cryptographic integrity check. It also provided secure authentication using pre shared keys or 802.1X.

RSN solves the problems in both WEP and WPA by using the CCMP for encryption and message integrity. The CCM mode of the AES cipher allows for both secure encryption and a cryptographic integrity check using a single key. Further improvements helped harden it against DoS attacks.

Though RSN is considered to be secure for the time being, but vulnerabilities are starting to appear. The CCMP attack reduces the key strength effectively making it easier to crack the pairwise transient and the Hole 196 allows for an authorized user to gain a significant measure of control over the system. They may need to be addressed for the standard to stay secure.

6 Recommendations

If it has not been done already, RSN should find a less predictable method of generating it's unique encryption nonce. The predictable nonce is a current vulnerability which can reduce the strength of the encryption. It could also by dealt with by improving the key size to 196 or 256 bytes. This would make the reduction by a third negligible and still produce strong encryption.

The RSN protocol should be expanded to allow for the verification of information sent from groupwise transient keys. This may be difficult as broadcast keys need to be shared with all authenticated clients in order to broadcast information. As AES is a symmetric cipher all clients are capable of encrypting and decrypting broadcast packets. If this was combined with a digital signature method, clients could discard any broadcast packets not digitally signed by the access point.

Future wireless security mechanisms or amendments to existing mechanisms, should have several key features in order to accomplish confidentiality, integrity and availability.

The first is strong encryption which does not reuse any initialization vector for the same or in the case of CCM, provide a predictable nonce. There should be no way for the key to be deduced. Also, the encryption should exhibit a strong avalanche effect as networking message may be extremely similar.

The second is a strong cryptographic integrity check. This should use a proven algorithm which is cryptographically secure hash function. Using a CRC-32 integrity check is not sufficient as an active attacker can easily calculate the required values. Likewise a strong avalanche effect is important to avoid an attacker deducing information from similar packets.

The third is denial of service protection. This appears to have been an afterthought in designing these security mechanisms. TKIP is introduces security features which make it relatively easy for an attacker to cause a a denial of service attack and originally RSN was vulnerable.

In the future is may be necessary to increase key sizes as computing power increases, as such security mechanisms should support larger keys than currently necessary.

Finally attacks seem to be continually improved. Small vulnerabilities are continually exploited until they become major vulnerabilities. Over time, techniques improve and new insights arise greatly increasing their efficiency; therefore, even small vulnerabilities should be fixed with care.

References

[1] W. A. Arbaugh, N. Shankar, Y. C. J. Wan, and K. Zhang. Your 802.11 Wireless Network has No Clothes. *IEEE Wireless Communications*, 9(6):44–51, 2002.

[2] M. Beck and E. Tews. Practical attacks against wep and wpa, November 2008.

[3] K. Benton. "the evolution of 802.11 wireless security", march 2010. "http://itffroc.org/pubs/benton_wireless.pdf".

[4] N. Borisov, I. Goldberg, and D. Wagner. Intercepting mobile communications: the insecurity of 802.11. In *Mo-*

biCom '01: Proceedings of the 7th annual international conference on Mobile computing and networking, pages 180–189, New York, NY, USA, 2001. ACM.

[5] F. M. Halvorsen and O. Haugen. Cryptanalysis of ieee 802.11i tkip. Master's thesis, Norwegian University of Science and Technology, June 2009.

[6] C. He and J. C. Mitchell. Security analysis and improvements for ieee 802.11i. In *In Proceedings of the 12th Annual Network and Distributed System Security Symposium*, pages 90–110, 2005.

[7] IEEE Computer Society, 3 Park Avenue, New York, NY 10016-5997, USA. *IEEE Std 802.11^{TM}-2007*, June 2007. pg. 158 - 160.

[8] IEEE Computer Society, 3 Park Avenue, New York, NY 10016-5997, USA. *IEEE Std 802.11^{TM}-2007*, June 2007. pg. 161 - 166.

[9] IEEE Computer Society, 3 Park Avenue, New York, NY 10016-5997, USA. *IEEE Std 802.11^{TM}-2007*, June 2007. pg. 212 - 215.

[10] IEEE Computer Society, 3 Park Avenue, New York, NY 10016-5997, USA. *IEEE Std 802.11^{TM}-2007*, June 2007. pg. 179 - 185.

[11] J. Jonsson. On the security of ctr + cbc-mac nist modes of operation - additional ccm documentation, 2002.

[12] M. Junaid and et al. Vulnerabilities of ieee 802.11i wireles lan . . ., 2006.

[13] T. Labs. Wpa cracker. http://www.wpacracker.com/index.html.

[14] T. Ohigashi and M. Morii. A practical message falsification attack on wpa, 2009.

[15] J. Wexler. Wpa2 vulnerability found. http://www.networkworld.com/newsletters/wireless/2010/072610wireless1.html.