**Critical issues in WEP which resulted in development of WPA in Wireless Network Security**

**1. Introduction**

We can define a wireless network as a type of computer network that uses wireless data connections for connecting to the network nodes. The major difference between wired and wireless networks is the way that how they transmit data. A wireless network uses radio waves to connect devices.

The implementation of wireless network takes place at the physical layer of the OSI model.

Examples of wireless networks include cell phone networks, Wireless local area networks (WLANs), wireless sensor networks, satellite communication networks, and terrestrial microwave networks [1].

Even though the wireless technology is fast, cost effective, flexible and easy to use. It poses serious security challenges and the choice of selecting a security protocol is a critical issue. Now, how to secure a wireless network from unauthorized access or damage to computers.

Many protocols /Algorithms like WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA 2 and RSN (Robust Security Network) were designed with the main goal to protect wireless network. In this paper, we mainly focus on what were the Issues with WEP that led to development of WPA and what was the need for WPA2.

# 2 IEEE 802.11 Standard [2]

IEEE 802.11 is a set of Wireless LAN standards developed by working group 11 of the IEEE 802 committee. The 802.11 standard was first released in 1997 and revised in 1999. When it comes to security, a number of committees have made an effort including the IEEE's 802.11 Task Group I (TGi), the Internet Engineering Task Force and the National Institute of Standards (NIST).

# 3. IEEE 802.11 Security

Since the data is broadcasted into the air, anyone within the interception range or having the right device can easily intercept the transmission. The 802.11 wireless network was designed with the intention to offer Security from eavesdropping, prevent unauthorized access to network (access control) and prevent tampering of transmitted messages [3]. To improve the security of a wireless system, many security mechanisms were developed.

# 3.1 Access Control List (ACL)

In general, we know that an ACL is a list which specifies which users or system processes are granted permission to access an objects or a file. This mechanism mainly focuses on filtering out unknown users and for this it requires a list of authorized client’s MAC addresses to be pre-loaded in the database. Only those registered MAC addresses will be able to communicate with the Access Point.

The disadvantage of this mechanism is that it just gives access to registered MAC addresses and rest will be dropped. But doesn't ensure confidentiality or integrity. Therefore, this mechanism is very

vulnerable and open to network attacks like MAC spoofing, Spoofing files (Race condition/ TOCTOU), Tampering with a file (Modifying ACL) etc. Easily.

# WEP (Wired Equivalent Privacy) - IEEE802.11

This was the first algorithm or protocol designed by IEEE's 802.11 to provide confidentiality and integrity to the wireless network. WEP uses CRC-32 algorithm for data integrity.

* + - WEP uses the RC4 stream cipher.
    - This RC4 stream cipher uses a 64bit key (40-bit WEP key (static part) with a 24-bit random number (dynamic part) known as an Initialization Vector (IV)) to encrypt the data.
    - The stream cipher with the plain text is XORed to produce ciphertext at the sender end.
    - The packet along with the IV and ciphertext is sent to the receiver.
    - The receiver decrypts the packet by performing a second logical XOR operation on its stored WEP key and the attached IV. This cancels the effect of the first logical XOR operation and the message is finally decrypted.
    - To synchronize the key of the sender and the receiver, the IV value is transmitted in plain text along with the data packet, here 24 bits of the 64 or 128 bits key is revealed.

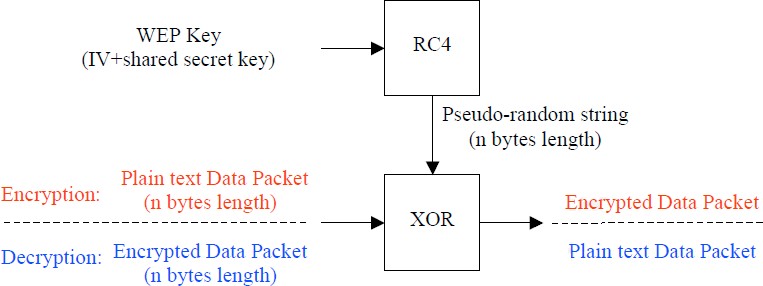


Figure 1. WEP Encryption/Decryption Process [3].

# 3.2.1 WEP Algorithm and its vulnerabilities

The application of WEP merely stopped casual sniffers but unfortunately experienced hackers could crack the WEP keys in a busy network within minutes.

WEP is considered as a broken protocol cause of its vulnerabilities like [4] [3] -

# WEP key recovery:

* + Weak IV – WEP uses same WEP key and different IV to encrypt the plain text (data). Due to RC4 implementation for encryption IV’s produce weak WEP key. Using a weak key is always risky. Let’s consider a scenario where the first few bytes of IV have some similarity with WEP key. Each key may leak at least one byte of secret key. For this attacker may have to capture huge amount of data. An attacker can study the IV’s to collect large data and if he gets to know that it’s repeated, this large data is enough to break WEP key. This weakness was first studied by Flusher, Mantin and Shamir and is published in their paper “weakness in the key scheduling algorithm in RC4” [6]. This is popularly known as FMS attack.

Also there are several WEP cracking tools available, this along with Brute forcing attacks is enough to obtain the shared secret key. Unauthorized decryption leads to violation of data integrity, once the key is compromised, the intruder may use the key to start sending messages to the receiver or might alter the ciphertext and forward modified message to the receiver and make the network defenseless.

* + Poor key management – There is no proper mechanism implemented to renew stored key. Once the key is compromised the key has to be changed. But in the large enterprise environment there will be 1000’s of wireless devices in the network ant it’s almost next to impossible to change them.
  + No proper access point authentication – Access point authentication is done by NIC’s but there is no mechanism for access point to authenticate NIC’s. Attacker may reroute the data to access points through alternate paths.

# IV Collision:

When an attacker uses this method he doesn't have to know the shared secret key and also there is no need of collecting huge amount of data.

We know that in WEP, IV has very limited range of keys to choose from. Eventually this leads to generation of same IV’s. An IV collision occurs when 2 or more are encrypted with the same IV and this leads to generation of same WEP key.

An attacker can use this to perform an XOR operation on 2 encrypted data packets. Here the encryption cancels out and results in revealing the plain texts. With more and more data packets having same WEP key this process of revelation becomes faster and faster. Also, eventually the attacker can keep all the pseudo random string in record and use it for decryption or forging of data packets.

# Weakness of ICV algorithm: [8]

To provide data integrity WEP uses CRC32- ICV. CRC32 is used to detect noise and common errors in the channel but it fails in cryptographic hash!

Attacker can easily modify the encrypted message and recalculate CRC and fix ICV and modify Access point to decrypt packets.

This can be easily done by taking the encrypted data packet and modifying the destination address of each packet to attackers IP address and then fixing the CRC and retransmitting it back to the access point and access point will definitely decrypt messages for the attacker.

# Dynamic WEP:

We know that the attacker needs to obtain large amount of data packets to break shared key. If the wireless network changes its key before the attacker gets enough packets to break the key then this will be much harder for attacker to crack the key.

So based upon this concept Dynamic WEP was developed. It involves generating a new WEP key regularly (time as set by system admin), after every fixed time interval the key gets refreshed. This mechanism uses authentication process. That is the authentication server generates WEP key only when the user is both authenticated and authorized.

But this mechanism failed because the attacker can monitor successful authentication and later forge it. Korek ChopChop attack [6] – this attack can be used to decrypt data packets without the

shared key. This attack reveals plain text without breaking the key. We know that a CRC32 – ICV is appended to data to protect the integrity of the data.

Access points can be used to differentiate between an encrypted packet with correct and incorrect checksum. When access point receives a packet from the unauthenticated client, error message is displayed and packet with incorrect checksum is discarded.

By using software’s such as aircrack-ng it is proved that if access points drop packets shorter than certain bytes, Airplay tries to guess the rest of the missing bits of the data. If an IP packet is captured it checks the header checksum and whether it’s correct after guessing missing parts to it. This attack worked majorly against Dynamic WEP [7].

# 3.3.2 Temporary Solutions

1. **Enhancement of WEP key –**

New key used 128 bit WEP. The WEP was extended from 40-bit to 104-bit for enhancing the security. The main intention was that attacker will take longer amount of tome to break the enhanced (extended) WEP key.

Unfortunately this was not helpful as the security flaws still existed and it was proved to be broken in less than a minute [5]

# Implementation of VPNs –

In the mechanism VPN hardware enabled the remote devices to establish secure connections to access points. In general, by using VPN encryption in addition to WEP encryption it is difficult for hacker to decipher the data twice. First WEP encryption and then VPN.

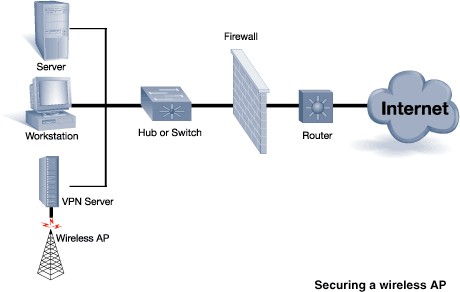


Figure 2. Using VPN for securing wireless AP [9]

But authentication mechanisms in VPN is weak if using PPTP, which transmits hashed passwords. In general, these temporary solutions also lead to poor interoperability in longer run and hence WEP is considered as a broken protocol.

# 3.3 WPA (Wi-Fi Protected Access)

When it was clear that WEP had some serious design issues and vulnerabilities IEEE Started developing WPA. It was designed and released by Wi-Fi Alliance as a solution for all known WEP vulnerabilities and targeted to increase the level of security for wireless networks until a definitive Security protocol was standardized. WPA Consisted of 3 main components TKIP, MIC and 802.1x.

WPA also used WEP's insecure RC4 stream cipher, but provided extra security through TKIP. There are two types of WPA -

1. Personal mode WPA – It has PSK authentication and TKIP/MIC encryption
2. Enterprise mode WPA – It has EAP authentication and TKIP/MIC encryption.

WPA includes following key features to address WEP vulnerabilities [4]:

* + Implements 802.1X EAP based authentication to enforce mutual authentication
  + Apply Temporal Key Integrity Protocol (TKIP) on existing RC4 WEP to impose strong data encryption
  + Use Michael Message Integrity Check for message integrity

# Temporary Key Integrity Protocol (TKIP) [9]

This protocol was used as a direct replacement to WEP as this overcame the most critical vulnerability of WEP. While designing this it was kept in mind that this should maintain compatibility with the existing hardware and could be implemented by just a software update. In this protocol each packet uses completely different key by generating it by using a per packet key mixing function.

Since mostly cryptographic parameters are hardcoded into the network interface hardware. Due to the limitation to ensure compatibility and performance to the hardware. WPA reused the hard coded functions like RC4 Stream cipher. But instead of using the shared secret key directly it used that as a seed to generate other keys which in turn minimized the risk of attacks on the shared secret keys.

# Working of TKIP.

The TKIP work is mostly based on the per packet key mixing function. In this per packet key mixing function is responsible for generating each packet’s key. Each key is generated by hashing÷≥÷≥÷/ Mac Address of the sender, The IV and the session key. In order to lower the amount of processing power to generate the key the Mixing Function is divided into two phases.

The first phase takes up most of the processor power. In this phase the Senders Mac Address, The temporal session key and the highest 32 bits of the IV are hashed together. This calculated value remains unchanged until a session change occurs or the session has ended or every time the IV uppers 32-bit change.

In the second phase the lower 16 bits of the packet and the result of phase 1 are hashed together. Which results in 104 bits per packet key. (Note: - This Phase is calculated for each packet which is received)

After the second phase the encryption process is similar to WEP. With the main differences being the WEP 24-bit IV Field being replaced by the WPA lower 16 bit IV with dummy byte inserted in Middle.

Also the WEP key is replaced by the per packet key in WPA. By using TKIP the encryption becomes effective 128-bit dynamic key rather than 24 bit dynamic with 104 bit static key. Which in turn increases the network security.

# Message Integrity Check (MIC) [4]

Message integrity check is a function in WPA which is responsible for the Integrity of the Data Packet. This is AN 8 byte value which is calculated on unencrypted data packet before encryption. The main motive of this function is to detect if any kind of modification was done during the transmission to the data packet. I.e. if the data packet was modified by some adversary during transmission or not.

The Hashing function which is being used in this was specially designed for hardware in network interfaces because of their low processing power. Also due to the fact that they have low power they kept the security protection equivalent to 20 bit key. Which is very low in terms of cryptographic security. But WPA consists of countermeasures which come in effect in case of a data packet modification attack

In case the Router detects and alteration in the message packet it then implements these countermeasures which is that the router disables the wireless link of all the compromised devices foe 60 seconds and every device is forced to request new session keys. But there is a drawback to these countermeasures which basically need to a Denial of Service attack. By forging invalid data packets which will make the router invoke these countermeasures continuously.

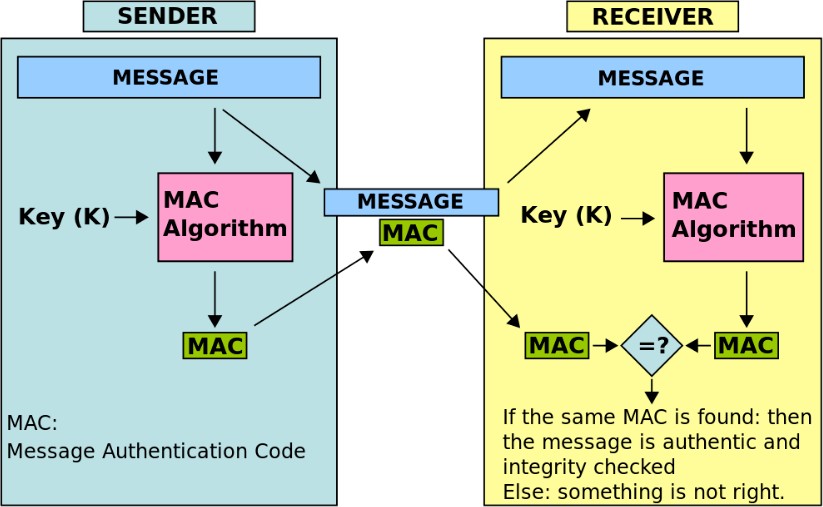


Figure 3. Message Authentication code algorithm

# 3.3.4 802.1x Port Based Network Access Control

* 1. x protocol was designed to protect network from user link like an access point in a wireless network. 802.1x standard is comprised of three elements
     + A Supplicant- it is the entity or the network client/user who want to connect to the network. These can be client software on a laptop or a mobile phone or a wireless device.
     + An Authenticator- It can be described as a link point where the supplicants physically connect to the network. Mostly this device is a network switch or an access point. This device basically acts as an intermediary between the supplicant and the authentication server relaying the authentication messages in-between.
     + Authentication Server- this is the authentication system where the client connected is validated, this can be any authentication server but mostly a RADIUS serve is used for this purpose.

In an 802.1x network if any client wants to connect and initiate a network session they must authenticate themselves before they actually get connected to the network. In this system the 802.1x switch or an access point will only let EAP (Extensive Authentication Protocol) authentication messages across and will block all other traffic including DHCP, HTTP, FTP, SMTP and POP3.

Until the authentication process is successfully complete. After this the authenticator transitions the supplicant port to an authorized state. WPA and 802.11 I uses this protocol in order to improve the

access control in the wireless network, this protocol is also responsible in providing the WPA session keys to the supplicant upon successful implementation.

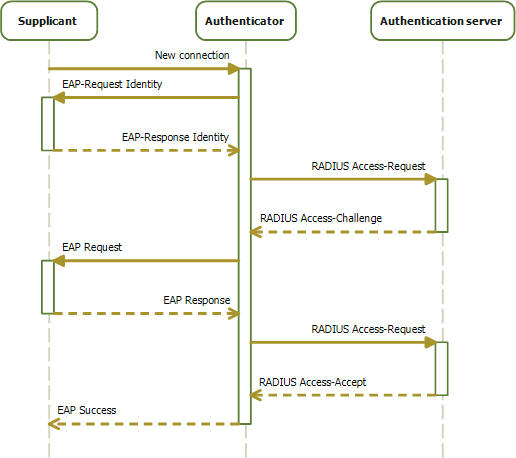


Figure 4. Sequence Diagram of 802.1X Progression [11]

## EAP (Extensible Authentication Protocol)

This protocol provides a generalized framework for a wireless network system to choose a specific method for authentication. There are different authentication method in the EAP system. For e.g. passwords, PKI certificates etc. The most common EAP methods which are used are in the following comparison chart taken from [12]:



Figure 5. Comparison between Different Commonly Used EAP Methods [13]

## 3.3.5 WPA-PSK (Pre shared Key)

WPA has a special mode in which it done not use the 802.1x Authentication method by using a pass phrase as a pre shared key. In this method every station may have its own pre shared key setup during the access point or router configuration and is tied up with its MAC address. In this configuration the user only needs to add a passphrase to the earlier WEP setting.

The weakness where this method fails is that if the pre shared key is set as a weak passphrase then the attacker can capture the authentication message and brute force it and recover the passphrase. The only solution to this is that the user should use a complex and long passphrase which should be a combination of uppercase lowercase numbers and special characters so that a dictionary or brute force attack could be avoided.

# WPA2- IEEE802.11i (The Ultimate Solution)

The 802.11i-2004 also known as the WPA2 is the main solution the IEEE committee gave for the vulnerabilities and design problems found in WEP. The WPA was a temporary solution to the WEP problems but WPA2 known as 802.11i standard is the ultimate solution to all those problems. This standard not only addresses the WEP problems but has also taken into account the future problems which may arise and have addressed them also.

The main difference between WPA and WPA2 is the mandatory use of Advanced Encryption Standard(AES) algorithms specified by NIST(National Institutes of standards and technology) to encrypt the data packets with the only downside of using the AES being that the old interfaces which used WEP could not be upgraded to support WPA2.

Also the WPA introduces the use of CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) as a replacement for TKIP.

There are two versions of WPA2. Personal mode WPA which has PSK authentication and AES/CCMP encryption. And an Enterprise mode WPA2 which has EAP authentication and AES/CCMP encryption.

# AES-CCMP (Advanced Encryption Standard- Counter Cipher mode with block chaining message authentication code protocol) [13]

This is an Encryption protocol designed for wireless networks which implement the 802.11i standard. This is an advanced encapsulation mechanism used for data confidentiality based on CBC-MAC mode of the AES standard. The AES algorithm is a basic block cipher which is used to encrypt the data in blocks of fixed lengths in case of 802.11i the size of the block used is 128-bit.

Since block ciphers has many modes by which they can split the data into fixed sixe block for encryption the operation mode also known as MOO used by WPA2 is CCMP (Counter mode with cipher block chaining message authentication code). This operation mode uses Counter mode for the privacy while the cipher block chaining message authentication code for data integrity and authentication

In this counter mode, each data block is not encrypted directly instead an arbitrary value is encrypted and then combined with a logical XOR with a data block and for every next data block the arbitrary value is incremented by one.

# RSN (Robust Security Network)

This is a protocol for establishing secure wireless communications in the 802.11i standard. This uses the authentication services and port access of the 802.1x for the establishment of cryptographic keys. RSN only allows the creation of robust security network associations (RSNAs). The initial authentication process is carried out by either using the PSK or by using the EAP exchange through 802.1x protocol. Once the authentication is completed a 4 way handshake take place in which the access point and the client independently prove to each other that they know PSK without ever disclosing the key.

The process works in this way that the client and the access point each encrypt messages to each other that can only be decrypted using the PSK they already have. Also we can say that the PSK acts an encryption/decryption key. If the decryption of the messages is successful it proves that both the client and the access point are genuine and know the PSK. The reason we use 4 way handshake is because it is critical for the protection from malicious access points/ routers.

The 4 way handshake is designed in such a way that it lasts an entire session and exposed very little. This handshake is used to establish another key called pairwise transient key (PTK). This PTK is generate by concatenating the PSK, AP nonce, STA nonce, AP mac, STA mac. And out through a PSR (Pseudo Random Generator). The below figure represents the working of the four way handshake in 802.11i.

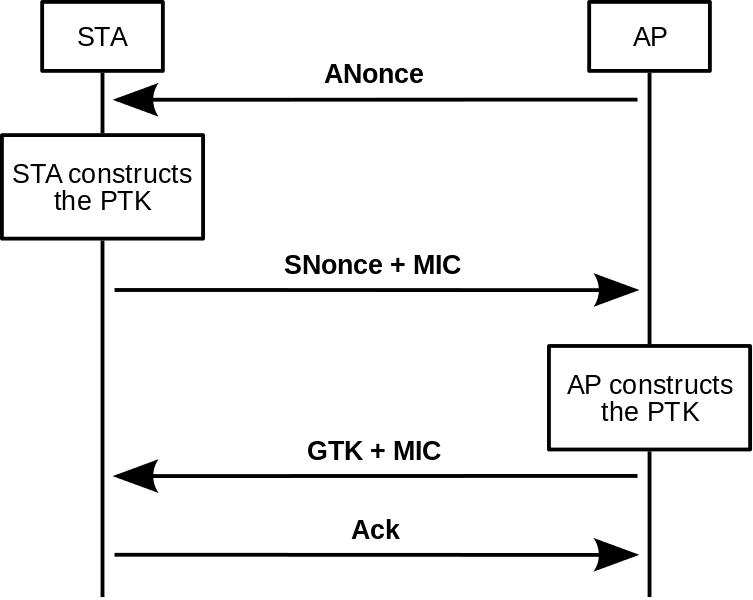


Figure 6. A Four-way Handshake in 802.11i [14]

# Conclusion [8] [15]

In this paper we briefly presented what were the problems in WEP, which made us shift to WPA and WPA2 and discussed the overall detail procedure for cracking WEP and WPA.

|  |  |  |  |
| --- | --- | --- | --- |
| Features | WEP | WPA | WPA2 |
| Stands For | Wired Equivalent Privacy | Wi-Fi Protected Access | Wi-Fi Protected Access 2 |
| Why was it introduced? | To provide data confidentiality comparable to a traditional wired Network. | For more security of Wireless networks. | Designed to replace the WEP and WPA protocols. |
| Method /Mechanism | It uses IEEE 802.11 algorithm and operates to create a wireless network that is equally strong as a wired net. | WPA uses WEP's insecure RC4 stream cipher, but with TKIP to provide more security | * WPA2 uses the AES instead of the RC4 stream cipher. * WPA's TKIP is replaced by CCMP |
| Keys | Static key | Temporary key – TKIP is used | User sets up the unique encryption key |
| Speed | Requires very little processing power | Requires little processing power | Requires greater processing power |
| Encryption Cipher | RC4 (Vulnerable – IV Usage) | RC4 / TKIP | AES / CCMP CCMP / TKIP |
| Encryption Key Size | 40 bits (104 bits was also used in some versions) | 128 bits | 128 bits |
| Encryption Key Management | NONE | 802.1x | 802.1x |
| Key Change | NONE | Each Packet | Not need |
| IV Size | 24 bits | 48 bits | 48 bits |
| Authentication | Weak | 802.1x – EAP | 802.1x -EAP |
| Data Integrity | CRC 32 – ICV | MIC (Michael) | CCMP |

Table-1. Summary comparison of WEP, WPA and WPA2 Security Protocols / algorithms. [8][15]

These comparisons made between security techniques shows the strengths and weaknesses of WEP, WPA and WPA2.

Wireless security has been undergoing major evolution in Past few years. The IEEE 802.11 Group, Wi-Fi Alliance and other major network equipment vendors are all working together to develop more secure standards.

WEP was regarded as a broken protocol in wireless security in 2001. The original WEP idea of using RC4 cipher is vulnerable because of insecure IV usage. The usage of 40 bits of encryption key, no proper key management mechanism, No periodic key change attribute, no header integrity, control mechanism and no replay attack prevention and easy capturing of small sized IVs has led to failure of WEP. The WEP was supposed to provide confidentiality and data Integrity as same level of wired networks but over the time it was found that it had serious security flaws that it was necessary to get a solution for it.

For an immediate fix to the issues in WEP IEEE gave a temporary solution known as WPA, WPA has numerous enhancements over WEP like added secrecy with TKIP encryption cipher mechanism, 128 bits of key size, mixed type of encryption key per packet usage, dynamic key management mechanism, more longer (48 bits) IV, EAP usage for authentication, data integrity and header integrity. WPA Provides both forward- and backward-compatible with present and future wireless standards. WPA Provides not only mobility and flexibility but also a security of data.

However, the recommended solution to WEP security problems was not WPA but is WPA2. Both WPA and WPA2 are much more secure than WEP but WPA was just an intermediate solution for backward compatibility with the existing network devices using WEP.

The ultimate solution given by IEEE for the issues in WEP is WPA2 also known as 802.11i. But there is one big issue with WPA2 is the backward compatibility, since WPA has different security implementation modes and if we want the full security features which WPA2 offers then there maybe cost considerations because the hardware change will be required due to the fact that WPA with AES is not supported on the older network devices (which supported the WPA and WEP). But if backward compatibility is the only thing required then the WPA mode with TKIP encryption standard should be used. As explained earlier the passphrase used for the security should be longer and should be a combination of uppercase, lowercase, number and special characters which will decrease the chance of brute forcing the passphrase. So it’s totally comes to the requirement of the user what the user wants. If he wants backward compatibility then the user should go with WPA which supports RC4 and maintains full compatibility with old Network hardware. But if user wants to have a taste of both the things then the WPA2 offers a feature called mixed mode which mixes some features of WPA and some of WPA2. The only drawback of this feature is that the load on the router increases which in turn slows down the whole network. But all in all I would say that if the user can afford to shift completely to WPA2 then the user should go in hands full on WPA2 using AES encryption scheme.

# References

1. https://en.wikipedia.org/wiki/Wireless\_network
2. Vishal Kumkar, Akhil Tiwari, Pawan Tiwari, Ashish Gupta, Seema Shrawne.Vulnerabilities of Wireless Security protocols (WEP and WPA2), ISSN: 2278 – 1323 International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 2, April 2012.
3. SANS Institute InfoSec Reading Room. An Overview of 802.11 Wireless Network Security Standards & Mechanisms.
4. Stanley Wong.The evolution of wireless security in 802.11 networks: WEP, WPA and

802.11 standards: GSEC Practical v1.4b, May 20, 2003.

1. Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin. Breaking 104 bit WEP in less than 60 seconds TU Darmstadt, FB Informatik Hochschulstrasse 10, 64289 Darmstadt, Germany
2. Martin Beck, Erik Tews. Practical Attacks Against WEP and WPA
3. ht[tps://www.aircrack-ng.org/doku.php?id=korek\_chopchop](http://www.aircrack-ng.org/doku.php?id=korek_chopchop)
4. Halil Ibrahim BULBUL, Ihsan BATMAZ, Mesut OZEL. Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols.
5. Attacks on the WEP protocol Erik Te[ws e tews@cdc.informatik.tu-darmstadt.de](mailto:tews@cdc.informatik.tu-darmstadt.de)
6. Vulnerabilities of Wireless Security protocols (WEP and WPA2) Vishal Kumkar, Akhil Tiwari, Pawan Tiwari, Ashish Gupta, Seema Shrawne
7. https://en.wikipedia.org/wiki/IEEE\_802.1X
8. <http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1300-> series/prod\_qas09186a00802030dc.html
9. https://en.wikipedia.org/wiki/CCMP
10. https://upload.wikimedia.org/wikipedia/commons/thumb/a/ac/4-way-handshake.svg/753px-4- way-handshake.svg.png
11. Tagwa Ahmed Bakri Gali, Amin Babiker A/Nabi Mustafa. A Comparative Study between WEP, WPA and WPA2 Security Algorithms: International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438 Volume 4 Issue 5, May 2015.