IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 6, Ser. I (Nov - Dec 2019), PP 25-32
www.iosrjournals.org

Security Analysis and Improvement for Wireless Security protocols

NagmdenMiled Naser[1], AdelAshour Abosdel[2], Nasser Bashir Ekreem[3]
1(Electrical and Computer Engineering ,Faculty of Engineering,AzzaytunaUniversity,Libya)
2(Electrical Engineering ,Faculty of Engineering,AzzaytunaUniversity,Libya)
3(Electrical Engineering ,Faculty of Engineering,AzzaytunaUniversity,Libya)
Corresponding Author: NagmdenMiled Naser

Abstract: *Wireless technology has been gaining rapidpopularity for some years. Adaptation of a standard dependson the ease of use and level of security it provides. In this case,contrast between wireless usage and security standards showthat the security is not keeping up with the growth paste of enduser's usage. Current wireless technologies in use allowhackers to monitor and even change the integrity oftransmitted data. Lack of rigid security standards has causedcompanies to invest millions on securing their wirelessnetworks ,There are three major types of security standards inwireless, Weexplained the structure of WEP and WPA as first and secondwireless security protocols and discussed all their versions, problems and improvements. Now, we try to explain WPA2versions, problems and enhancements that have done solve theWPA major weakness. Finally we make a comparison amongWEP and WPA and WPA2 as all wireless security protocols inWi-Fi technology. In the next phase we hope that we willpublish a complete comparison among wireless securitytechniques by add the WiMax security technique and make awhole comparison among all security protocols in this area.*

Keywords: *Wireless Security, WEP, WPA, WPA2, 802.11i*

Date of Submission: 22-11-2019 Date of Acceptance: 06-12-2019

I. Introduction

The 802.11 WLAN standardsspecify the two lowest layer of the OSI network modelwhich are physical and data link layers. The major goals ofIEEE for creating these standards were made differentapproach to the physical layer, for example differentfrequencies, different encoding methods, and share the samehigher layers[8].

They have succeeded, and the Media AccessControl (MAC) layers of the 802.11a, b, and g protocols areconsiderably identical. At the next higher layer still, all802.11 WLAN protocols specify the use of the 802.2protocol for the logical link control (LLC) portion of the datalink layer. As you can see in Figure1,In the OSI model ofnetwork, such protocols as TCP/IP, IPX, NetBEUI, and AppleTalk, still exist at higher layers. Each layer utilizes theservices of the underside layers. Figure1 In WLANs, privacy is achieved by data contentsprotection with encryption. Encryption is optional in 802.11WLANs, but without it, any other standard wireless device, can read all traffic in network. There have been three majorgenerations of security approaches, which is mentionedbelow:

- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fa Protected Access)
- WPA2/802.11i (Wi-Fa Protection Access, Version 2),Each of these protocols has two generations named aspersonal and enterprise template[5].

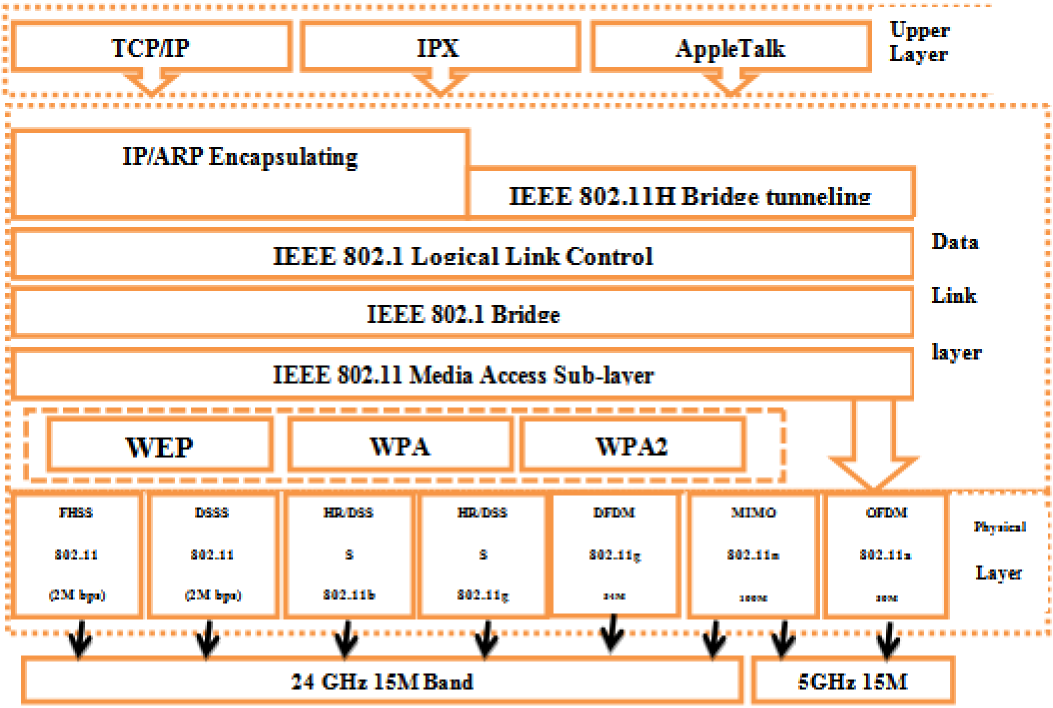

Figure1: 802.11 And OSI Modell

II. WEP Static or Personal

The Wired Equivalent Privacy (WEP) was designed toprovide the security of a wired LAN by encryption throughuse of the RC4 algorithm with two side of a datacommunication.

In the Sender Side

WEP try to use from four operations to encrypt the data(plaintext).At first, the secret key used in WEP algorithm is40-bit long with a 24-bit Initialization Vector (IV) that isconcatenated to it for acting as the encryption/decryption key. Secondly, the resulting key acts as the seed for a Pseudo-Random Number Generator (PRNG).Thirdly, the plaintextthrow in a integrity algorithm and concatenate by theplaintext again. Fourthly, the result of key sequence and ICVwill go to RC4 algorithm. A final encrypted message is madeby attaching the IV in front of the Cipher text. Now inFigure2,define the objects and explain the detail ofoperations[1].

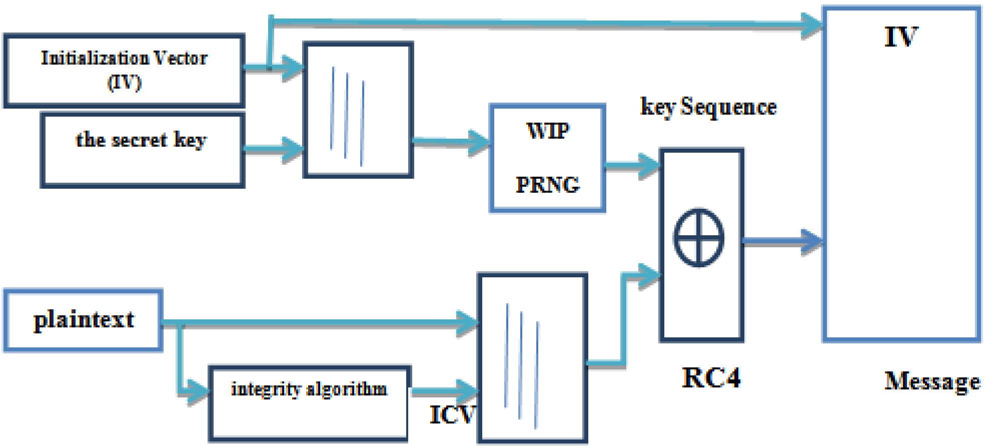

Figure 2: WEP Encryption Algorithm (Sender Side)

In the Recipient Side

WEP try to use from five operations to decrypt thereceived side (IV+Cipher text).At first, the Pre-Shared Keyand IV concatenated to make a secret key. Secondly, theCipher text and Secret Key go to in CR4 algorithm and aplaintext come as a result. Thirdly, the ICV and plaintext willseparate. Fourthly, the plaintext goes to Integrity Algorithmto make a new ICV (ICV') and finally the new ICV (ICV')compare with original ICV. In Figure3,you can see theobjects and the detail of operations schematically [2].

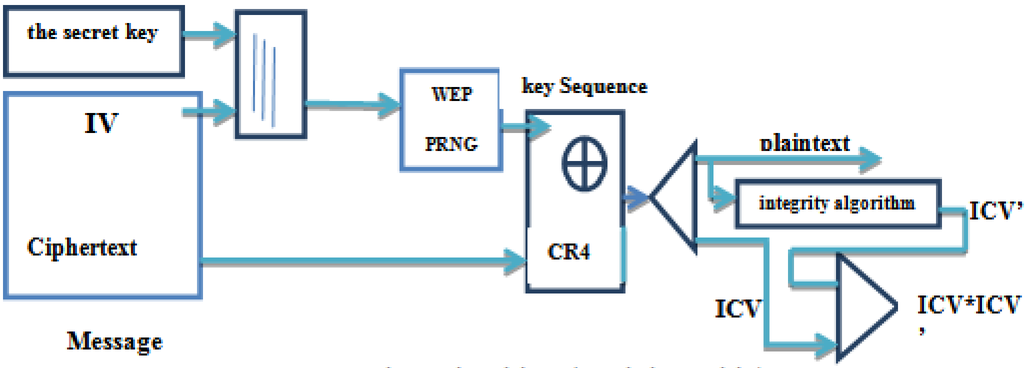

Figure3: WEP Decryption Algorithm (Recipient Side)

There are some other implementations of WEP that all ofthem are non-standard fixes and implemented by somecompanies. I will explain 3 of them here:

WEP2:This stopgap enhancement to WEP was present in someof the early 802.11i drafts. It was implement able on some(not all) hardware not able to handle WPA or WPA2, andextended both the IV and the key values to 128 bits. It washoped to eliminate the duplicate IV deficiency as well as stopbrute force key attacks. After it became clear that the overallWEP algorithm was deficient however (and not just the IVand key sizes) and would require even more fixes, both theWEP2 name and original algorithm were dropped. The twoextended key lengths remained in what eventually becameWPA's TKIP.

WEP plus: WEP+ is a proprietary enhancement to WEP by AgreeSystems (formerly a subsidiary of Lucent Technologies) thatenhances WEP security by avoiding "weak IVs", It is onlycompletely effective when WEP plus is used at both ends ofthe wireless connection. As this cannot easily be enforced, itremains a serious limitation. It is possible that successfulattacks against WEP plus will eventually be found. It alsodoes not necessarily prevent replay attacks[9].

Dynamic WEP:Change WEP keys dynamically. Vendor-specific featureprovided by several vendors such as 3Com. The dynamicchange idea made it into 802.11i as part of TKIP, but not forthe actual WEP algorithm.

WEPWeaknessesand Enhancements

We explain about problems and solutions onWEP, finally we can found these results from our previousarticle:

• WEP does not Prevent forgery of packets.
• WEP does not prevent replay attacks. An attacker cansimply record and replay packets as desired and theywill be accepted as legitimate.
• WEP uses RC4 improperly: The keys used are veryweak, and can be brute-forced on standard computers inhours to minutes, using freely available software.
• WEP reuses initialization vectors: Avariety of availablecryptanalytic methods can decrypt data without knowingthe encryption key.
• WEP allows an attacker to undetectably modify amessage without knowing the encryption key.
• Key management is lack and updating is poor.
• Problem in the RC-4 algorithm.
• Easy forging of authentication messages.

And we found these Enhancements over WEP in that article:Improved data encryption (TKIP), User authentication (UseEAP Method) and Integrity Michael Method[1].

Now we try to explain the WPA structure and discussabout problems and improvements on it.

III. WPA Personal or Commercial

The WPA came with the purpose of solving the problemsin the WEP cryptography method, without the users needs tochange the hardware. The standard WPA similar to WEPspecifies two operation manners:

1. Personal WPA or WPA-PSK (Key Pre-Shared) that usefor small office and home for domestic useauthentication which does not use an authenticationserver and the data cryptography key can go up to 256bits. Unlike WEP, this can be any alphanumeric stringand is used only to negotiate the initialsession with theAP. Because both the client and the AP already possessthis key, WPA provides mutual authentication, and thekey is never transmitted over the air.
2. Enterprise WPA or Commercial that the authenticationis made by an authentication server 802.1x, generatingan excellent control and security in the users' traffic ofthe wireless network. This WPA uses 802.1X+EAP forauthentication, but again replaces WEP with the moreadvanced TKIP encryption.

No preshared key is usedhere, but you will need a RADIUS server. And you getall the other benefits 802.1X+EAP provides, includingintegration with the Windows login process and supportfor EAP-TLS and PEAP authentication methods.The main reason why WPA generated after WEP is thatthe WPA allows a more complex data encryption on theTKIP protocol (Temporal Key Integrity Protocol) andassisted by MIC (Message Integrity Check) also, whichfunction is to avoid attacks of bit-flipping type easily applied WEP by using a hashing technique. Refer to the Figure2 and Figure3 you can see the wholepicture of WEP processes in sender and receiver sides[6], nowwe draw a whole picture of WPA process Figure4.

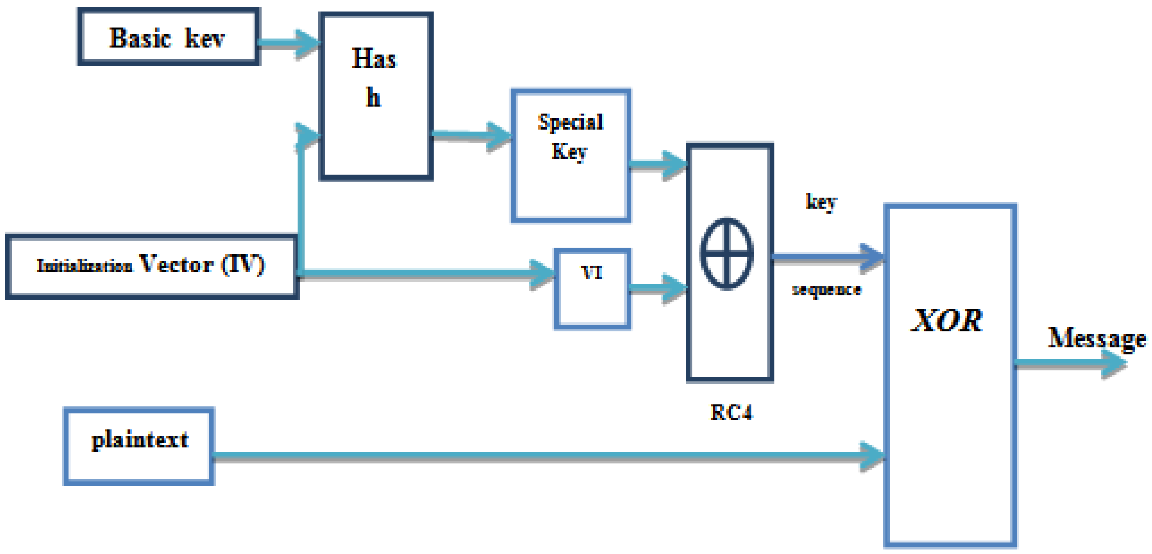

Figure 4: WPA Encryption Algorithm (TKIP)

As you see, TKIP uses the same WEP's RC4 Technique,but making a hash before the increasing of the algorithmRC4.A duplication of the initialization vector is made. Onecopy is sent to the next step, and the other is hashed (mixed)with the base key, After performing the hashing, the result generates the keyto the package that is going to join the first copy of theinitialization vector, occurring the increment of the algorithmRC4. After that, there's the generation of a sequential keywith an XOR from the text that you wish to cryptograph,generating then the cryptography text. Finally, the message isready for send. It is encryption and decryption willperformed by inverting the process[4].

.WPA Improvements

In the comparison between TKIP and WEP there are fourimprovements in Encryption algorithm of WPA that added toWEP:

1. Acryptographic message integrity code, or MIC, calledMichael, to defeat forgeries.
2. A new IV sequencing discipline, to remove replayattacks from the attacker's arsenal.
3. A per-packet key mixing function, to de-correlate thepublic IVs from weak keys.

4.A rekeying mechanism, to provide fresh encryption andintegrity keys, undoing the threat of attacks stemmingfrom key reuse. Now we explain these four algorithms one by one:

MIC **or Michae**

Michael is the name of the TKIPmessage integrity code, It is an entirely new MIC designedthat has 64-bits length and represented as two 32-bit little-Endian words ($K0$,$K1$).The Michael function first pads amessage with the hexadecimal value 0x5a and enough zeropad to bring the total message length to a multiple of 32-bits,then partitions the result into a sequence of 32-bit words $M1M2\ldots Mn$, and finally computes the tag from the key and themessage words using a simple iterative structure:words using a simple iterative structure:

$(L,R) \leftarrow (K0,K1)$

do i from 1 to n

$L \leftarrow L \text{ XOR } Mi$

$(L,R) \leftarrow \text{Swap}(L,R)$

return (L,R) as the tag

TheMichael verification predicate reruns the taggingfunction over the message and returns the result of a bit-wisecompare of this locally computed tag and the tag receivedwith the message[3].

The security level of a MIC is usually measured in bits. Ifthe security level of a MIC is s bits, then, by definition, thetime required for an attacker to construct a forgery is, onaverage, after about $2\text{-}s+1$packet.New IV sequencing discipline For Defeating Replayed:One forgery a MIC cannot detect is a replayed packet, This occurs when an adversary records a valid packet inflight and later retransmits it.To defeat replays, TKIP reuses the WEP IV field as apacket sequence number. Both transmitter and receiverinitialize the packet sequence space to zero whenever newTKIP keys are set, and the transmitter increments thesequence number with each packet it sends.

TKIP requiresthe receiver to enforce proper IV sequencing of arrivingpackets. TKIP defines a packet as out-of-sequence if its IV isthe same or smaller than a previous correctly receivedMPDU associated with the same encryption key, If anMPDU arrives out of order, then it is considered to be areplay, and the receiver discards it and increments a replaycounter[12].

Key Mixing

As you saw in Figure1 and Figure2 WEP constructs a per-packetRC4 key by concatenating a base key and the packetIV, The new per-packet key that called the TKIP key mixingfunction substitutes a *temporal key* for the WEP base keyand constructs the WEP per-packet key in a novel fashion, Temporal keys are so named because they have a fixedlifetime and are replaced frequently.The mixing function operates in two phases:

• Phase 1 eliminates the same key from use by all links:Phase 1 combines the 802 MAC addresses of the localwireless interface and the temporal key by iterativelyXORing each of their bytes to index into an S-box, toproduce an intermediate key, Stirring the local MAC addressinto the temporal key in this way causes different stationsand access points to generate different intermediate keys,even if they begin from the same temporal key-a situationcommon in ad hoc deployments. This construction forces thestream of generated per-packet encryption keys to differ atevery station, satisfying the first design goal, The Phase 1 intermediate key must be computed only whenthe temporal key is updated, so most implementations cacheits value as a performance optimization.

• Phase 2 de-correlates the public IV from known theper-packet key: Phase 2 uses a tiny cipher to encrypt the packet sequencenumber under the intermediate key, producing a 128-bit per-packetkey. Actuality, the first 3 bytes of Phase 2 output areexactlymach to the WEP IV, and the last 13 to the WEPbase key, as existing WEP hardware expects to concatenate abase key to an IV to form the per-packet key. This designaccomplishes the second mixing function design goal, bymaking it difficult for a rival to be connected to IVs and pay-packetkeys, Rekeying or Defeating key collision attacks: Rekeying delivers the fresh keys consumed by thevarious TKIP algorithms. Generally there are three key types:temporal keys, encryption keys and master [12].

Occupying the lowest level of the hierarchy are thetemporal keys consumed by the TKIP privacy andauthentication algorithms proper. TKIP employs a pair oftemporal key types: a 128-bit encryption key, and a second64-bit key for data integrity. TKIP uses a separate pair oftemporal keys in each direction of an association. Hence,each association has two pairs of keys, for a total of fourtemporal keys. TKIP identifies this set of keys by a two-bitidentifier called a *WEP key id*. Now we can drawing a newfigure from TKIP process with details of these fourparts. Figure5.

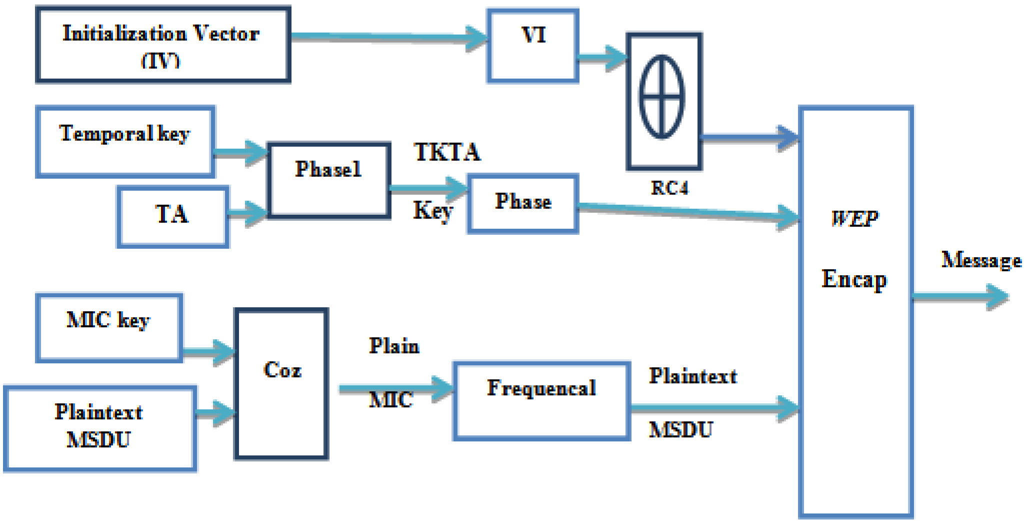

Figure 5: TKIP Detail Encryption Algorithm

WPAWeaknesses

In November 2003, Robert Moskowitz released"Weakness in Passphrase Choice in WPA Interface". In thispaper he explains a formula that would reveal the passphraseby performing a dictionary attack against WPA-PSKnetworks.

This weakness was based on the pairwise masterkey (PMK) that is derived from the concatenation of thepassphrase, SSID, length of the SSID and nonces (a numberor bit string used only once in each session). The result stringis hashed 4,096 times to generate a 256-bit value and thencombine with nonce values. The required information forgenerate and verify this key (per session) is broadcast withnormal traffic and is really obtainable; the challenge thenbecomes the reconstruction of the original values. Heexplains that the pairwise transient key (PTK) is a keyed-HMAC function based on the PMK; by capturing the four way authentication handshake, the attacker has the datarequired to subject the passphrase to a dictionary attack[12].

Finally he found that "a key generated from a passphrase ofless than about 20 characters is unlikely to deter attacks.For confirmation, in late 2004, Takehiro Takahashi, thena student at Georgia Tech, released WPA Cracker and JoshWright, a network engineer and well-known security lecturer, releasedcowpatty around the same time. Both tools arewritten for Linux systems and perform a brute-forcedictionary attack against WPA-PSK networks in an attemptto determine the shared passphrase. Both require the user tosupply a dictionary file and a dump file that contains theWPA-PSK four-way handshake. Both function similarly;however, cowpatty contains an automatic parser while WPACracker requires the user to perform a manual stringextraction. Additionally, cowpatty has optimized theHMAC-SHA1 function and is somewhat faster. Each tooluses the PBKDF2 algorithm that governs PSK hashing toattack and determine the passphrase. Neither is extremelyfast or effective against larger passphrases, though, as eachmust perform 4,096 HMAC-SHA1 related to the values asdescribed in the Moskowitz[11].

IV. WPA2 Personal or Enterprise

The 802.11i standard is virtually identical to WPA2, andthe terms are often used interchangeably 802.11i and WPA2are not just the future of wireless access authentication – theyare the future of wireless access. Wireless access is still in itsinfancy, in spite of the purchase and deployment of severalmillion access points and wireless clients. The majority ofthese access points and clients are relatively immobile. Userssit down with their laptops at a conference table and connect,or a clerk stays within a relatively small area such as awarehouse, using wireless equipment to track inventory[10].

WPAwas provided as an interim solution, and it had anumber of major constraints. WPA2 was designed as afuture-proof solution based on lessons learned by WEPimplementers. Motorola is a key contributor and proponentof the WPA2 standard, and provides next generationproducts based on this standard[8].

WPA2 will be a durable standard for many reasons. Oneof the most important choices was that of the encryptionalgorithm. In October 2000, the National Institute ofStandards and Technology (NIST) designated the AdvancedEncryption Standard (AES) as a robust successor to theaging Data Encryption Standard. AES is an extremely welldocumented international encryption algorithm free ofroyalty or patent, with extensive public review[7].

WPA2, like WPA, supports two modes of security,sometimes referred to as “*home user* “and corporate.*” Inhome user*” mode a pre-shared secret is used, much likeWEP or WAP. Access points and clients are all manuallyconfigured to use the same secret of up to 64 ASCIIcharacters, such as “*thisisoursecretpassword.*” An actual256-bit randomly generated number may also be used, butthis is difficult to enter manually into client configurations, The“*corporate*” security is based on 802.1X, the EAPauthentication framework (including RADIUS), one ofseveral EAP types (such as EAP-TLS, which provides amuch stronger authentication system), and secure keydistribution. “Homeuser “security introduces the samesecurity problems present in WEP and WPA-PSK. Here weexplain *“corporate*”security, In security algorithm of 802.11i providing key enablerfor secure and flexible wireless networks, allowing for clientauthentication, wireless network authentication, keydistribution and the pre-authentication necessary for roaming. In using 802.1X in conjunction with 802.11i, it is stronglysuggested to use EAP as a framework for authentication, anduse an EAP type for the actual authentication that providesthe optimal balance between cost, manageability and riskmitigation. Most often an802.1X setup uses EAP-TLSforauthentication between the wireless client (supplicant) andthe access point (authenticator),In theory, several optionsmay replace EAP-TLS, butin practice this is[8].

In 802.1X, no such port exists until the client connectsand associates to the wireless access point. This immediatelyposes a problem, since beacon packets and proberequest/response packets cannot be protected orauthenticated. Fortunately, access to this data is not veryuseful for attackers, other than for potentially causing denial of-service attacks, and for identifying wireless clients andaccess points by their hardware MAC addresses ,An 802.1X wireless setup consists of three maincomponents:

• Supplicant (the wireless client).
• Authenticator (the access point).
• Authentication server (usually a RADIUS server).

The supplicant initially connects to the authenticator, as itwould to a WEP- or WPA protected network. Once thisconnection is established, the supplicant has in effect anetwork link to the authenticator (access point). Thesupplicant can then use this link to authenticate and gainfurther network access. The supplicant and authenticator firstnegotiate capabilities. These consist of three items:

• The pairwise cipher suite, used to encrypt unicast(point-to-point) traffic.
• The group cipher suite, used to encrypt multicast andbroadcast (point-to-multiple points) traffic.
• The use of either a pre-shared key (PSK, or “*homeuser*” security, using a shared secret) or 802.1Xauthentication.

So, the main problem of WPA as a pairwise solved bydivided the type of security to three categories witch just inone of them use pairwise and in two other use group cipherand pre-shared key[3].

V. Conclusion

At first, we explain the structure of WEP in sender andreceiver side and describe all steps verbally and practically atthe same time, Secondly, we discuss about the second generation ofwireless security protocol as WPA and define the two modesand try to describe all major Improvements on WPA such ascryptographic message integrity code or MIC, new IVsequencing discipline, per-packet key mixing function andrekeying mechanism then make a whole diagram for WPAencryption and decryption. Finally, explain about the majorproblem on WPA that happed in the PSK part of algorithm. Finally, we discuss about third generation of wirelesssecurity protocol as WPA2/802.11i and define two type ofthis security as home user and corporate. Then we explainthe improvement that has done in this protocol for solve theWPA major problem. This is done by categorize the securityto three groups and use group cipher and pre-shared key. We hope as continues papers in the next paper we willexplain the WiMax and make a totally survey on wirelesssecurity protocols and try to design a whole diagram ofsecurity protocols and completely discuss on weaknessesand improvements of them[7].

Acknowledgments

We would like to express our appreciation to our parentsand all the teachers and lecturers who help us to understandthe importance of knowledge and show us the best way togain it.

Refrences

[1]. Arash Habibi Lashkari, F. Towhidi, R. S. Hoseini, “Wired EquivalentPrivacy(WEP)”, ICFCC Kuala Lumpur Conference, 2009
[2]. Arash Habibi Lashkari, MasoodMansoori, Amir SeyedDanesh;“Wired Equivalent Privacy(WEP) versus Wi-fi Protected Access”, ICCDA Singapore Conference, 2009
[3]. Donggang Liu, P. N., “Security for Wireless Sensor Networks”,Springer., November, 2006
[4]. Garcia, R. H. a. M., “AN ANALYSIS OF WIRELESS SECURITY”,CCSC: South Central Conference. 2006
[5]. Kempf, J., “Wireless Internet Security: Architecture and Protocols“,Cambridge University Press. October, 2008
[6]. Hani Ragab Hassan, YacineChallal, “Enhanced WEP: An efficientsolution to WEP threats”, IEEE 2005

[7]. Halil Ibrahim BULBUL, Ihsan BATMAZ, Mesut OZEL,"Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network)Security Protocols"; e-Forensics January 2008, Adelaide ,Australia.

[8]. Arunesh Mishra, William, A. Arbaugh, "An Initial Security Analysisof The IEEE 802.1X Standard", University of Meryland, 2002

[9]. Vebjørn Moen, H˚avardRaddum, Kjell J. Hole; "Weaknesses in theTemporal Key Hash of WPA"; Mobile Computing and Communications Review,2005

[10]. John L. MacMichael ; "Auditing Wi-Fi Protected Access (WPA)Pre-Shared Key Mode"; Linux Journal, 2005

[11]. Bhagyavati, Wayne C. Summers, Anthony DeJoie;"Wireless SecurityTechniques: An Overview"; InfoSec Conference, September 2004

[12]. Yoshiaki Hori , Kouichi Sakurai ;"Security Analysis of MIS Protocolon Wireless LAN comparison with IEEE802.11i ";Mobility Conference , October 2006, Thailand

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Nagmden Miled Naser. " Security Analysis and Improvement for Wireless Security protocols" IOSR Journal of Computer Engineering (IOSR-JCE) 21.6 (2019): 25-32.