WIRELESS SECURITY PROTOCOLS (WEP,WPA,WPA2 & WPA3)

V.Srikanth[1], Dr. Indira Reddy[2]
Department of Information Technology
Sreenidhi Institute of Science and Technology, Hyderabad, 501301, India.

Abstract : Wireless networks have posed a threat in Data Security that has stuck to the core of data communication between two points. Absence of inflexible security measures has made numerous organizations contribute millions to verify their systems. Development of different security conventions for Wireless LANs has been given in this paper. Also, vulnerabilities of WEP/WPA/WPA2/WPA3 have been discussed and how the wireless networks are attacked using the design flaws present in these Wireless Security Protocols. The use of different tools and programming languages used for testing the strength of the protocols. Tools like nmap, zenmap, aircrack-ng, etc., are used in the Linux environment to practically demonstrate the attacks against these networks using WEP/WPA/WPA2/WPA3 protocols. The solutions for the shortcomings in WEP has been applied in WPA, similarly WPA2 and WPA3.

IndexTerms **- Equivalent Privacy, Wi-Fi Protected Access, TKIP (Temporal key Integrity Protocol), CCMP (Counter mode with Cipher block Chaining Message Authentication Code), SAE (Simultaneous Authentication of Equals).**

I. INTRODUCTION

IEEE characterized 802.11 Wireless LAN Standards, expected to enable remote association of workstations to their base LAN.WLAN application speaks to a developing specialty in the market, the innovation on which it is based begun to be utilized additionally for another application, that of conveying Broadband Wireless Access (BWA) to open systems.The primary reason for making IEEE Standards were made in a diverse way to deal with the physical layer like various frequencies and distinctive encoding strategies.WLAN conventions indicate the utilization of 802.2 for sensible connection control (LLC) segment of the data link layer. In WLANs, security is accomplished by encrypting the information.Without Encryption, some other remote devices can sniff the traffic in the system. The three noteworthy security methodologies are referenced underneath:

- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access)
- WPA2 (Wi-Fi Protected Access, ver 2)

WEP (Wired Equivalent Privacy)

WEP is intended to give security of wired LAN by encryption, utilizing RC4 algorithm with different sides of information correspondence.

SENDER'S SIDE:

WEP utilizes four operations to encode and send the information. In initial step secret key is utilized in WEP calculation is 40-bit along with 24-bit Initialization Vector (IV) which is concatenated to act as both encryption and decryption key. In the second step, the subsequent keys go about as a seed for Pseudo-Random Generator (PRNG). In the Third Step, plaintext checks for uprightness by a calculation and link by the plain content once more. In the last step, the result of the key sequence and ICV will go to the RC4 algorithm, encoded message is framed by joining the Initialization Vector before the Cipher text.

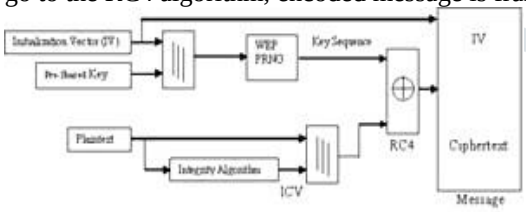

Figure 1: WEP encryption Sender side

RECIPIENTS SIDE:

WEP utilizes five tasks to decrypt (IV+cipher text). Firstly, the Pre-Shared key and IV are linked to make a secret key. In the Second step, Cipher text and Secret Key go to CR4 algorithm and plain text comes as a result. In the third step, the ICV and plain text will isolate. Fourthly, the plaintext goes for integrity check to make another ICV and compares with original ICV.

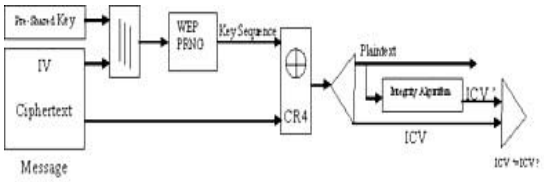

Figure 2: WEP encryption Receivers side

WPA(Wi-Fi Protected Access)

It was presented by Wi-Fi alliance in late 2002. Wi-Fi Alliance with Electronics Engineers (IEEE) secured the feeble sections of the recently disclosed WEP protocol and presented WPA as an interpretation. It has been made compatible with all vendors and existing equipment. The primary concern is to defeat WEP shortcoming without the change in equipment. This was finished by

including (TKIP) Temporal Key Integrity Protocol for encryption and 802.1X EAP for authentication purpose to offer high security. To keep away from Information Fabrication (bit flipping), WPA presented Message Integrity Check (MIC) calculation known as "Michael".

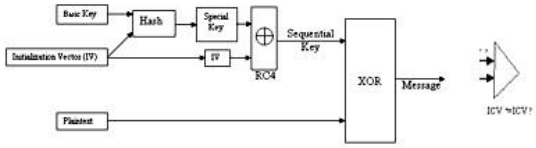

Figure 3: WPA Encryption Algorithm (TKIP)

WPA2(Wi-Fi protected Access 2)

Implements totally IEEE 802.11 standard and improvement over WPA. Furnishes information protection by counter mode with cipher block chaining message Authentication Code Protocol (CCMP) utilizing Advanced Encryption Standard (AES) block cipher. Uses WPA2-Personal and WPA2-enterprise for Authentication. Information Integrity is checked by means of Cipher Block Chaining message validation. Secures against Replay assaults by 48-bit packet number.

CCMP Encryption Process:

- For every Medium access control Protocol Data Unit (MPDU) there is a packet number (PN) and this number will be increased for each next MPDU.
- In the header of MPDU, there is something which refers to as Additional Authentication
- Data (AAD) and in this field the integrity conveyed by CCMP is addressed to.
- To make the CCMP Nonce prevent the PN and, A2 (MPDU address 2) and Priority field of MPDU will be utilized. The Priority field has stored the value of zero.
- In extension, the new PN along with the key identifier collectively will be employed to fabricate the 64-bit CCMP header.
- The nonce, group of temporal key, AAD and MPDU information are utilized to make the cipher and MIC.
- The encryption of MPDU is acquired by consolidating the CCMP header, unique MPDU header, encrypted data, and MIC.

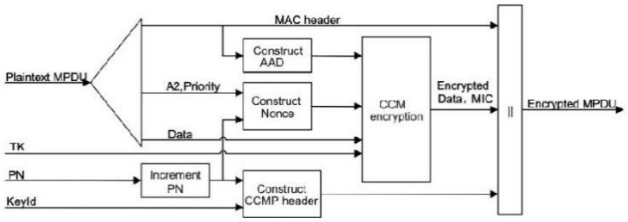

Figure 4:CCMP Encryption

CCMP Decryption Process:

•Later the encoded MPDU is acquired, the AAD and nonce values could be extracted from the encrypted MPDU.

•The header of the encoded MPDU is employed to make the AAD.

•To make the nonce, the estimations of various fields of the header will be utilized which are thePN, MPDU address 2 (A2), and Priority fields.

•To recoup the MPDU plaintext, AAD, temporal key, MIC, nonce and MPDU cipher text are consolidated together. Besides now the integrity of MPDU and AA plaintext is affirmed.

•Finally, by incorporating MAC header of MPDU and decoded MPDU plaintext, the Plaintext of MPDU is decrypted

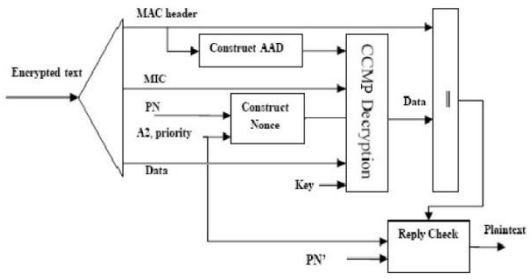

Figure 5:CCMP Decryption

WPA3 (Wi-Fi Protected Access 3)

Wi-Fi union impelled WPA3 the cutting edge remote security standard that can dispose of every current defencelessness. The key highlights of WPA3 are Protection against brute force attacks, WPA3 Secrecy, Protecting Open/Public Networks. WPA3 utilizes SAE (Simultaneous Authentication of Equals) handshake to offer Forward Secrecy, which keeps the offender from decoding old caught traffic. Gives individualized data encryption a component that encodes remote traffic to alleviate the danger of Man-in-the-Middle-Attacks. Provides 192 -bit encryption to Wi-Fi associations.

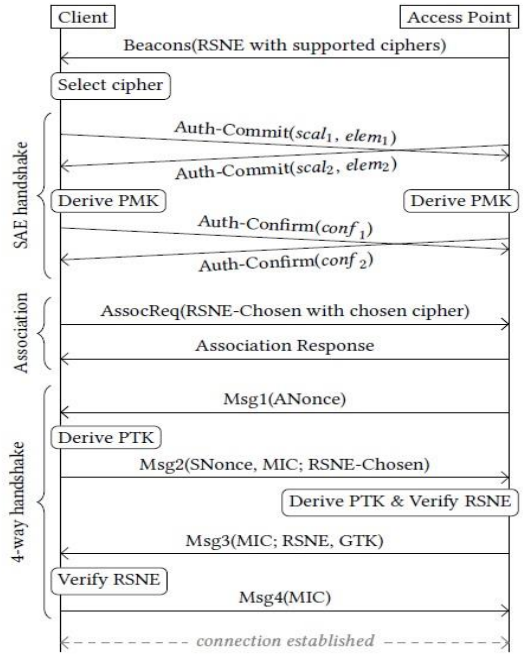

Figure 6: SAE Handshake

II. LITERATURE REVIEW

Arash Habibi Lashkari [1] discussed in his paper about the structure of WEP the versions of it and the weakness of WEP. The author explained main weakness of WEP are RC4 algorithm because of its short IV size, key management, Elementary forging of Authentication messages and advances of WEP can be performed by using TKIP.
S.Vinjosh Reddy [2] explained about cracking WEP encryption of Wi-Fi networks So as to know about the tools used and to strengthen our Wi-Fi.

Cracking WEP:

- Client encrypts data using a key
- Encrypted packets are sent in the air
- Router Decrypts packets using the key

Every packet is encrypted utilizing a special key stream.
Random Initialization Vector (IV) is employed to create the key stream. The initialization vector is only 24 bits.
Enable monitor mode.
Capture a large number of packets/IVs using airodump-ng.
Analyse the captured IVs and crack the key using aircrack-ng.
If the network is too busy it may take more time to capture enough IVs.So,force the access point to generate new IVs.
WEP Cracking ARP Request replay

- Wait for an ARP packet
- Capture it, and replay it.
- This causes the AP to produce another packet with a new IV.
- Continue doing this till we have enough IVs to break the key.

Arash HabibiLashkari [3] compared WEP with WPA.The author defined WEP weakness and enhancements, WPA improvements

WEP Weakness:

- WEP does not anticipate the fabrication of packets.
- WEP does not anticipate replay attacks. An attacker can basically record and replay packets as wanted and they will be acknowledged as authentic.
- WEP employs RC4 inappropriately. The keys utilized are frail and can be brute-forced on standard PCs in hours to minutes, utilizing available accessible programs.
- WEP reuses initialization vectors. An assortment of accessible cryptanalytic techniques that can decode information without obtaining the encryption key.
- Without detection, WEP enables an attacker to change the information without obtaining the encryption key.
- Key administration is insufficient and refreshing is poor.
- The issue in the RC-4 algorithm.
- Simple producing of authentication messages.

Enhancements over WEP:

- Improved data encryption (TKIP)
- User authentication (Use EAP Method)
- Integrity (Michael Method)

Arash Habibi Lashkari [4] gave detailed explanation on WEP,WPA and explained the weakness and improvements. Likewise, WPA2 versions, issues, and improvements that are done to explain significant shortcoming in WPA, the correlation among WEP, WPA, WPA2 security protocols.
WPA Improvements.

- Cryptographic message integrity code to overcome reproductions.
- New IV sequencing system for Defeating Replay attacks.
- Per Packet Key mixing capability, to de-correspond the public IVs from feeble keys.
- Re-keying or defeating key collision attacks.

SamiaAlblwi [5] gave an overview of WPA2 and discussed about how vulnerabilities present in WEP and WPA are fixed. Weakness of WPA2 are also discussed in this paper. Yonglei Liu [6] presented attacking methods of WPA/WPA2.Strategies like Brute force, TMTO brute force attacks, Brute forcing utilizing GPU, TKIP key mixing Function, TKIP Beck&Tews, CCMP TMTO attacks are unmistakably simplified.

NorazaidiBaharudin [7] referenced that management frames on 802.11 a/b/g/n were sent in decoded plain content, thus can be fooled and fabricated simply by the intruder. Wireless Intruder Detection System (WIDS) is intended to shield the wireless clients from the de-authentication and disassociation attacks. WIDS screens beacon frames and differentiate the SSID of the AP and the relegated authentic AP.

Hacking WPA/WPA2 network:

- Enable monitor mode
- Capture the 4 way handshake
- The handshake doesn't contain any data that helps recover the key.
- It contains data to check whether a key is lawful or not
- The given 4 way handshake is compared with a wordlist

Cracking Wi-Fi password using PMKID:

- This method doesn't require to capture handshake.
- An attacker can employ a tool, as hcx dump instrument (v4.2.0 or higher), to challenge the PMKID from the targeted access point and dump the got frame to a record.
- Appropriating the hcx cap tool, the output of the frame would then be able to be changed over into a hash format acknowledged by Hashcat.
- Use Hashcat (v4.2.0 or higher) secret key cracking tool to get the WPA PSK (Pre-Shared Key) secret key.
- Decrypting may require some time relying upon its length and complexity.

MathyVanhoef [8] proposed an attack that misuses the flaws in protocols to reuse and reinstall an as of now being used key. For a fruitful attack the offender needs to fool the person into re-installing already in use key, when the victim reinstalls this key related parameters like the incremental transmit packet number (i.e nonce) and receive packet number (i.e replay counter) are reset to their original value. Basically, to ensure security, a key should just be introduced and utilized once. Unfortunately, discovered this isn't ensured by the WPA2 protocol.

WPA2 Vulnerabilities

- Reinstallation of the Pairwise Encryption Key (PTK-TK), Group Key (GTK), Integrity Group Key (IGTK) in the four-way handshake.
- Reinstallation of the STK key in the Peer Key handshake and Tunnelled Direct-Link Setup (TDLS) Peer Key (TPK) in the TDLS handshake.
- Reinstallation of the Group Key (GTK) and Integrity Group Key(IGTK) while handling a Wireless Network Management (WNM) Sleep Mode Response frame.

Dr.Pandi Kumar [9] incorporated the examination of the diverse encryption strategies for standard WEP and WPA2. The main point of the investigation is to have a better knowledge of how excellent security protocols are utilized, how communication channel is defended, how validation is taken care of, how information is encrypted and at last perks and vulnerabilities of every protocol.

BabitaDagar [10] concentrated on the advancement of Wireless LANs and correlation has been given between the protocols. Since WPA2 is the most adopted protocol for wireless systems at present so its constraints are talked about.

Mahmoud Khasawneh [11] portrayed the protocols, such as WPA and WPA2. WPA gives client security and privacy by utilizing TKIP for encryption and Michael for data integrity. Despite the improvements given by WPA, it has some shortcomings with respect to the authentication and data integrity process. New component for data integrity in WPA2 was proposed which is CCMP.
Vipin Poddar's [12] paper is a near investigation of WEP, WPA, and WPA2. To check the authentication of all protocols by suggesting the legendary attack vector scripts i.e Air crack set of tools. The test discovered that WEP is weakest, to which WPA was an impermanent method and WPA2 is strong with long haul adjustment.

Muthu Pavithran [13] plans to transmit a wireless penetration test and compares the encrypted key of a wireless network with a document that contains the captured packets. Additionally penetration tests in WEP and WPA/WPA2 protocols and furthermore the techniques to build up these protocols employing different attacks.

Kirti Rana [14] thinks about WEP and WPA encryption mechanism for better knowledge of their working standards and security bugs. How security protocols validate the clients? How simple it is to break the security protocols of wireless systems with a set of tools. Utilization of aircrack-ng and comm-view tool to demonstrate methods for hacking.

Ashish Garg [15] proposed adjustment to the first RC4 algorithm to make it progressively secure and much quicker, increment the span of initial vector without expanding the general size of the 64-bit session key employed in WEP and giving an outline to dynamically change the secret key before getting any plausibility to breaking the secret key from the scrambled data packets.

Pranav S.Ambavkar [16] portrayed the shortcoming of "Solid WPA/WPA2 Authentication" and perceive that it is so straightforward to break the protocol. New standard's WPA and WPA2 executions alongside their first minor vulnerabilities and how it is conceivable to break.

Tomoaki Sato [17] proposed an agreeable WEP algorithm to which cipher strength is increased using algorithm and software implementation due to which processing rate of compatible WEP algorithm is more high-speed than that of traditional WEP algorithm.

MathyVanhoef [18] indicated how WPA3 is influenced by a few design flaws and review these defects both hypothetically and practically. Clarified how Simultaneous Authentication of Equals otherwise called Dragonfly is influenced by password partitioning attacks. Likewise referenced how to alleviate their attacks in a backward-compatible way and how minor changes to the WPA3 protocol could have counteracted most of their attacks. The contributions made are:

- Pointed out how anti-clogging mechanisms of SAE is unable to shield denial-of-service attacks.
- Violating the overhead of SAE's defenses upon already-known side-channels, a resource-constrained device can load the CPU of a known Access Point (AP).
- Performed dictionary attack against WPA3 when it is running in transition mode this is done by downgrading the clients to WPA2 and also downgrade attack against SAE.
- Empirically studied the probability of timing attacks against WPA3's SAE handshake and validated timing attacks are possible and can disclose information about the password.
- Theoretically and practically how the recovered timing and cache info can be used to implement an offline password partitioning attack which facilitates an adversary to retrieve the password used by the victim.

III. CONCLUSION

In this review paper various Wireless Security protocols like WEP/WPA/WPA2/WPA3 are discussed. At first overview of WEP is given and how the attacks take place in WEP based networks can be seen. Secondly, the improvements made to WPA/WPA2/WPA3 to overcome all types of attacks are discussed. Vulnerabilities of each protocol and the improvements over the preceding are mentioned. Though the drafting of Wireless Security Protocols is done very efficiently and productively still there are some vulnerabilities which are seen after the implementation due to which there may be some cost restrictions or hardware restrictions to apply the patches or replace the equipment. So, the conclusion of this paper is that the security issues must be carefully kept in mind while designing the Wireless Security Protocols as the hackers are discovering new ways to engage. Also, we must hack our systems so as to point out the loopholes in our network and cover them before anyone attacks.

REFERENCES

[1] Arash Habibi Lashkari, F. Towhidi, R. S. Hoseini, "Wired Equivalent Privacy(WEP)", ICFCC Kuala Lumpur Conference, Published byIEEE Computer Society, Indexed by THAMSON ISI, 2009.
[2] S.vinjosh Reddy, K.Rijutha, K.Sai Ramani, Sk Mohammad Ali, CH.Pradeep Reddy, "Wireless Hacking - A WiFi Hack By Cracking WEP", 201O 2nd International Conference on Education Technology and Computer (ICETC)
[3] Arash Habibi Lashkari, Masood Mansoori, Amir SeyedDanesh "Wired Equivalent Privacy (Wep) Versus Wi-Fi Protected Access (Wpa)"2009 International Conference On Signal Processing Systems
[4] Arash Habibi Lashkari, Mir Mohammad SeyedDanesh, BehrangSamadi,"A Survey on Wireless Security Protocols(WEP, WPA and WPA2/802.11i)
[5] SamiaAlblwi, Khalil Shujaee,"A Survey on Wireless Security Protocol WPA2",Int'l Conf. Security and Management | SAM'17 |
[6]Yonglei Liu, ZhigangJin, Ying Wang, "Survey on security scheme and attacking methods of WPA/WPA2"
[7] NorzaidiBaharudin, Fakariah HaniMohd Ali, Mohamad Yusof Darus, Norkhushaini Awang, "Wireless Intruder Detection System (WIDS) in Detecting De-Authentication and Disassociation Attacks in IEEE 802.11"
[8] MathyVanhoef, Frank Piessens," Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2"
[9] Dr.T.Pandikumar1, Mohammed Ali Yesuf,"Wi-Fi Security and Test Bed Implementation for WEP and WPA Cracking"
[10] BabitaDagar, Neha Goyal," Integrating Enhanced Security Measures in WEP/WPA/WPA2-PSK"
[11] Mahmoud Khasawneh, IzadeenKajman, RashedAlkhudaidy, and Anwar Althubyani," A Survey on Wi-Fi Protocols:WPA and WPA2"
[12] Vipin Poddar, Hitesh Choudhary," A Comparitive Analysis Of WirelessSecurity Protocols (Wep And Wpa2)"
[13] Muthu Pavithran. S, Pavithran. S**,"** Advanced Attack Against Wireless Networks Wep, Wpa/Wpa2-Personal AndWpa/Wpa2-Enterprise"
[14] Kirti Rana, Aakanksha Jain, "Comparison and Analysis of Existing Security Protocols in Wireless Networks"
[15] Ashish Garg," A Novel Approach to Secure WEP by Introducing an Additional layer over RC4"

[16] Pranav S. Ambavkar, Pranit U. Patil, Dr.B.B.Meshram, Prof. Pamu Kumar Swamy," WPA Exploitation In The World Of Wireless Network"
[17] Tomoaki Sato, PhichetMoungnoue, and Masa-akiFukase," Compatible WEP Algorithm for Improved Cipher Strength and High-Speed Processing"
[18] MathyVanhoef, Eyal Ronen, "Dragonblood: A Security Analysis of WPA3's SAE Handshake"
[19] Arif Sari, Mehmet Karay," Comparative Analysis of Wireless Security Protocols: WEP vs WPA"
[20] V.A.A.S.Perera, E.A.M.K.B.Ekanayake, S.S. Shurane, P.A.IsuruUdayanga, J.P.Maharajage, R.M.C.Bandara, DhishanDhammearatchi,"Enhancement WPA2 protocol with WTLS to certify security in large scale organizations inner access layer Wi-Fi media associated devices"
[21] Kashish Monga, Vishal Arora, Ashish Kumar, "Analyzing the behavior of WP A with modification", 2015 IEEE International Conference on Communication Networks (ICCN)
[22] Jose Perez, "A Survey Of Wireless Network Security Protocols.