National Conference on
"Role of Engineers in Nation Building" organized by VIVA Institute of Technology, Mumbai
(6th and 7th March 2020)
International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

LAYERS OF WI-FI SECURITY

Nishant Pimple[1], Utkarsha Pawar[2], Tejashree Salunke[3]
Computer Engineering Department, Mumbai University, MUMBAI.
[1]jiten.nish@gmail.com, [2]utkarshapawar2299@gmail.com,
[3]tejashrees04@gmail.com.

Abstract- *Today's home network may include a wide range of wireless devices from computers, phones cameras, smart tv's and connected appliances. In today's era, the probability of getting hacked has grown extensively. Taking basic steps to secure your home network will help protect your devices and information. There is no awareness among people about security mechanisms. The current security protocols are not that strong to protect users from getting hacked. From the past experiences study reveals that router security encrypted protocol can be cracked using several ways like dictionary and brute force attacks. These methods are costly, require extensive hardware, not reliable and do not detect all the vulnerabilities of the system. In the proposed system we aim to test all Wi-Fi protocols which are WEP, WPA, WPA2 and WPS and provide prevention methods for detected credulity. It aspires to create an accurate and useful analysis of network standards and will suggest ways to improve these networks. In this system, we are going to look at a few of the different network related securities that have come along since the introduction of the wireless local area network (WLAN) and their various weaknesses. Wi-Fi access is very important in our life, but we need security at public and private levels of usage. The system we create will be efficient, portable and detect all the flaws. It analyses a variety of different network encryptions and how to breach said networks by majorly maintaining the confidentiality of user's personal data. The system will analyse the security mechanism of the router and fix the vulnerabilities and safeguard the router.*

Keywords- WEP,WLAN,WPA,WPA/2,WPS.

I. INTRODUCTION

The system analyzes a variety of different network encryptions and how to breach said networks. It aspires to create an accurate and useful analysis of network standards and will suggest ways to improve these networks. Upgrades will be made utilizing investigation into the branch of knowledge. Each systems administration encryption standard (WPA/WPA2, WPS) will likewise be completely talkedabout.

In the framework, the system related protections that have tagged along since the introduction of the Wireless Local Area Network (WLAN) and their different shortcomings are thought about. Predominantly the themes talked about will shift from the open encryption to non-encryption techniques which rely upon programming encryption(https, etc...) to protect data, along with the easily broken Wired Equivalent Privacy (WEP) and then the Wi-Fi Protected Access (WPA) followed by the Wi-Fi Protected Access II (WPA2). Proper procedures for maintaining high levels of security in order to keeptheuserprotectedwillbeexploredanddiscussed.Themostpromisingfeatureaddedinthedeviceis"portability".

The system aims to study ethical hacking of Wi-Fi networking encryption protocols. It is made for educational purpose only and aims in bringing awareness among society about the privacy of their respective data and how they can safeguard their data from intruders/crackers.

II. LITERATURESURVEY

Radhi S Nair, et.al [1] did the predetermined review on a few Wi-Fi Security strategies that makes a presentation of new answers for Wi-Fi security. This paper depicts numerous strategies for security strategy in Wi-Fi and determines favorable circumstances of these techniques. An overview on strategies, for example, AP security for Wi-Fi, Fog figuring, conventional Wi-Fi security techniques.

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

Dongsheng Yin, et.al [2] proposed a framework where the objective is check the individuals' keenness through research on the security of the WLANs around us. He completely broke down the inert shortcoming of WLANs' both encryption modes- - WEP and WPA\WPA2, lastly proposed a progression of successful answers for WLAN.

Dr. Glen Sagers, et.al [3] analyzed the relation between remote passages gathered through wardriving and a progression of United States Census socio/economic factors in two networks. They found critical relationships between Wi-Fi security race/ethnicity, which may likewise connect to instruction levels and pay. They likewise proposed that a more prominent mindfulness and additionally producer driven default security for remote passages ought to be important to guarantee better security.

Austin Gilbert, [4] examined the remote systems administration's presentation into the commercial center joining the advantages of client accommodation and business economy to fuel its mind boggling development. He found that remote systems are found wherever from the biggest global organizations to the smallest home workplaces. He additionally gave the investigation of the presentation of interesting security challenges for organized security experts and manages the same for remote systems administration.

Andrew Zafft, et.al [5] dissected city-level Wi-Fi security insights for eighteen urban communities inside the United States. They found that overall, 45 percent of Wi-Fis considered were shaky, with Miami, FL having 81 percent of Wi-Fi systems unbound. They additionally found a few urban communities with a high number of boycotted IP addresses. At last, they found no solid relationship between Wi-Fi weakness rates and boycotting rates, which ascribe to deficient training of the occupants of urban areas on the most proficient method to report pernicious movement with the goal that culprits can be boycotted. At long last, the level of secure Wi-Fi arranged in urban areas with city Wi-Fi systems was practically identical to that of urban areas without metropolitan Wi-Fisystems.

Ranjini Mukhopadhyay, et.al [6] exhibited the methods how a client can forestall his/her PC from any assault of any programmer. She gave a thought regarding moral hacking otherwise called infiltration testing or white-cap hacking that includes similar devices, stunts, and procedures that programmers use. Moral hacking is performed with the objective's authorization. The goal of moral hacking is to find vulnerabilities from a programmer's perspective so frameworks can be better verified. It is a piece of a general data chance administration program that takes into consideration continuous security upgrades. Moral hacking can likewise guarantee that sellers' cases about the security of their items areauthentic.

Maryna Yevdokymenko, et.al [7] contemplated moral hacking so as to characterize, dissect, talk about and resolve the absolute generally normal and broadly spread dangers and their functionalities as indicated by which vulnerabilities are as of now at hands in most risk occurrences and attempt to thought of new methods to progressively powerful settling of such issues.

Haishen Peng, [8] examined vulnerabilities, clarified the mainstream security innovation, proposed comprehensive reaching measures to determine WI-FI organize security, set forward WI-FI network fundamental security setup program, moderate security design program and propelled security design program just as planned for helping WI-FI arrange client to set up a safe system application stage.

S Vinjosh Reddy, et.al [9] understood the random dangers and vulnerabilities related with 802.11-based remote systems and morally hacking them to make them progressively secure. On this fragment, he held onto a glance at regular dangers, vulnerabilities related with remote systems and furthermore examined the whole procedure of splitting WEP (Wired Equivalent Privacy) encryption of Wi-Fi, focusing the need to get comfortable with checking devices like Cain, NetStumbler, Kismet and MiniStumbler to help study the area and tests that should run in order to reinforce our air signals.

Saif Ur Rehman, et.al [10] first presented and basically explored various potential strategies for automatic key refreshing and afterward proposed a dynamic key administration procedure. The proposing strategy works at the application layer. It is a

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

computerized encryption key update strategy that can fundamentally improve the security of WEP without requiring any adjustments in the standard or at the lower layers of the OSI model.

Yonglei Liu, et.al. [11] proposed a framework that gives us an overview of WPA/WPA2. And then, the vulnerabilities of WPA/WPA2 and current research in the strategy for assaulting WPA/WPA2 are presented. The design intent of WPA/WPA2 is to fix the flaws of WEP in order to defeat forgery attack, replay attack, weak-key attack, etc, and reinforcement the security of WLAN.

Chia-Mei Chen, et.al [12] examined that there is a security hole by the social human variables which are the powerless passwords. He additionally found that beast power secret phrase assaults are utilizing word reference records that are erraticand amazingly work. Thus, he proposed 10 guideline based strategies which are universally comprehensive and socially selective and demonstrate the instability of WPA and WPA2 by 100 observational and significant genuine remote scrambled parcels of WPA and WPA2. The proof shows that there is a 68 % breaking rate and afterward do the secret word designs examination also.

Omar Nakhila, et.al [13] built up another plan to accelerate the dynamic pass-express speculating preliminaries force dependent on two original thoughts. The plan impersonates different Wi-Fi customers associating with the AP simultaneously, each imitated Wi-Fi customer has its own MAC address. Each copied Wi-Fi customer could attempt many pass-phrases utilizing a solitary remote session without the need to pass the 802.11 validation and affiliation stages for each pass-expression surmise. They have built up a working model and investigations show that the proposed plan can improve dynamic word reference pass-express speculating speed by 100-overlay contrasted with the conventional single customer assault.

III. ANALYSIS

The following table is a summary of various research papers on Wi-Fi security techniques.

TABLE 1
ANALYSIS

SR. NO.	TITLE	TECHNIQUES USED	DRAWBACKS	OPEN CHALLENGES
1	A SURVEY ON WI-FI SECURITY TECHNIQUES[1]	Temporal key integrity protocol, counter mode with cipher block chaining message authentication code protocol, CCMP	Security of WPA/WPA2 is threatened.	As the inherent defect protocol WEP is insecure. Some vulnerabilities can be used by attackers to attack.
2	A RESEARCH INTO THE LATENT DANGER OF WLAN [2]	Four way- Handshake packets,	Disastrous consequences may happen, WEP encryption is weak and Risky.	Indecipherable under limited computation capability.

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

3	WHERE'S THE SECURITY IN WI-FI? AN ARGUMENT FOR INDUSTRY AWARENESS [3]	War driving.	As Wi-Fi use increases, even current levels of encryption use leave large amounts of personal information vulnerable.	In short, the problem of lack of Wi-Fi encryption represents an open challenge to the computing community.
4	WIRELESS SECURITY STUDY GUIDE: MEDIOCRE AT BEST [4]	WLAN auditing tools.	Insecurity levels of WI-FI networks.	Wireless networking introduces unique security challenges for network security professionals and administratorsalike.
5	MALICIOUS WI-FI NETWORKS: A FIRST LOOK [5]	AnalysisMethodology, Data Manipulation Methodology, DataAcquisition Methodology.	Wireless Networking Introduces Unique Security Challenges for Network Security.	Better tools for localizing IP addresses are needed.
6	ETHICAL HACKING: SCOPE AND CHALLENGES IN THE 21ST CENTURY [6]	Operating-system attack, distributed denial of service attacks (ddos).	We should be careful when we are performing the ethical hacking tests. It is not practical to make sure that no hackers are on our system.	If a user does not have a lot of foot traffic in the office and no internal web server running, the user may not have as much to worry about as an internet hosting provider would have.
7	ETHICAL HACKING AND PENETRATION TESTING USING RASPBERRY PI [7]	Passive reconnaissance, active reconnaissance.	Although active reconnaissance produce more information and more useful information, interactions with the target system may be logged, triggering alarms by protective device, such as firewalls and intrusion detection systems. As the usefulness of the data to the attacker increase, so does the risk of detection	patches can be put into places to reinforce your network defense

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

8	WI-FINETWORK INFORMATION SECURITY ANALYSIS RESEARCH [8]	Data encryption, WEP data encryption technology, network resource access technology.	Encryption algorithm, are too simple. WEP is easy to crack keys by attackers.	Network access control, data confidentiality, data integrity, protection.
9	WIRELESS HACKING - A WI-FI HACK BY CRACKING WEP [9]	Wired network back door entry points	Need to test wireless arrangements. Since the security harms with the 802.11 protocol weren't adequate, we have to be anxious about operating systems and utilities on wireless-client machines readily vulnerable to exploit.	Encryption flaws has been discovered which needs to be solved.
10	ON ENHANCING WEP SECURITY AGAINST BRUTE-FORCE AND COMPROMISED KEYS [10]	Dynamic key management, MAC authentication, public key cryptography.	Number of attempts should be put in wait period to validate key	No build in provision for particular standards.
11	SURVEY ON SECURITY SCHEME AND ATTACKING METHODS OF WPA/WPA2 [11]	Brute force attack, TMTO brute force attack, Brute force attack using GPU, TKIP key mixing function attack, TKIP Beck&Tews attack, CCMP TMTO attack.	As discovered vulnerabilities, the security of WPA/WPA2 is threatened.	It is also concluded that when designing a security protocol, security should kept in mind from the very beginning.
12	THE CRYPTANALYSIS OF WPA & WPA2 IN THE RULE BASED BRUTE FORCE ATTACK, AN ADVANCED AND EFFICIENT METHOD [12]	Cryptanalysis WPA and WPA2, wireless security.	Encryption is tough	Complex stuffed algorithm.
13	PARALLEL ACTIVE DICTIONARY ATTACK ON WPA2-PSK WI-FI NETWORKS [13]	Active Dictionary Attack, WPA2-PSK key generation.	WPA2-PSK does not limit the number of trials a wireless client can take to enter the pass-phrase.	limiting the number and the speed of pass-guessing trials will significantly.

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

IV. CONCLUSION

There are numerous ways for the data to be undermined and so as to decrease the danger of data falling into an inappropriate hands; security is required. In spite of that there isn't a way to deal with making the data 100% secure, whether or not it is straightforward or propelled; it very well may be made hard to get by others. The system addresses ethical hacking from several perspectives. Moral hacking is by all accounts another popular expression despite the fact that methods and thoughts of testing security by assaulting an establishment aren't new in any way. The study of cracking protocols to test the security mechanism of a router and to fix the vulnerabilities and safeguard the confidentiality of the user is the objective.

REFERENCES

[1] Radhi S Nair, Prof. Ashok Babu, Dr. Vinodh P Vijayan, "A Survey on Wi-Fi Security Techniques", International Research Journal of Engineering and Technology (IRJET),Volume: 05 Issue: 04, Apr-2018, pp 4705 -4707.
[2] Dongsheng Yin and Kai Cui, "A Research into The Latent Danger of WLAN", The 6th International Conference on Computer Science & Education (ICCSE 2011), August 3-5, 2011, pp 1085 –1090.
[3] Dr. Glen Sagers, Dr.Bryan Hosack, Dr. RJ Rowley, Dr. Douglas Twitchell, Ms. Ranjitha Nagaraj, "Where's the Security in Wi-Fi? An Argument for Industry Awareness", 2015, 48th Hawaii International Conference on System Sciences, pp 5453-5461.
[4] Austin Gilbert, "Wireless Security Study Guide: Mediocre at Best", IEEE DISTRIBUTED SYSTEMS ONLINE 2005 Published by the IEEE Computer Society, Vol. 6, No. 11, November 2005, pp 1 -3.
[5] Andrew Zafft and Emmanuel Agu, "Malicious Wi-Fi Networks: A First Look", 7th IEEE Workshop on Security in Communication Networks 2012 SICK 2012, Clearwater" pp1038-1043.
[6] RanjiniMukhopadhyayandAsokeNath,"EthicalHacking:Scopeandchallengesin21stcentury",InternationalJournalof InnovativeResearchinAdvancedEngineering(IJIRAE)ISSN:2349-2163,Volume1Issue11,November2014,pp30–37.
[7] MarynaYevdo,NymenNo,ElsayedMohamed,PaulOnwuaNpaArinze,"EthicalHackingandPenetrationTestingUsing Raspberry PI", 2017 4th International Scientific-Practical Conference Problems of Info-communications, October10-13, 2017, pp 1791-84.
[8] Haishen Peng, "WI-FI network information security analysis research" 2012 IEEE, pp 2243 –2245.
[9] S Vinjosh Reddy, K SaiRamani, K Rijutha, Sk Mohammad Ali, CR. Pradeep Reddy, "Wireless Hacking - A Wi-Fi Hack By CrackingWEP",20102ndInternationalConferenceonEducationTechnologyandComputer(ICETC)",2010,pp189-193.
[10] Saif Ur Rehman, Saeed Ullah, Sardar Ali, "On Enhancing the WEP Security Against Brute-force and Compromised Keys", 2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM), 2010, pp 250 -254.
[11] Yonglei Liu, Zhigang Jin, Ying Wang, "Survey on security scheme and attacking methods of WPA/WPA2", 2010 IEEE, pp 10-13.
[12] Chia-Mei Chen and Tien-Ho Chang, "The Cryptanalysis of WPA & WPA2 in the Rule-Based Brute Force Attack", An Advanced and Efficient Method 2015 10th Asia Joint Conference on Information Security, 2015, pp 37 –41.
[13] Omar Nakhila, Afraa Attiah, Yier Jin, Cliff Zou, "Parallel Active Dictionary Attack on WPA2-PSK Wi-Fi Networks", 2015 Track 3 - Cyber Security and Trusted Computing, 2015, pp 665 –670.