Ethical Hacking of IEEE 802.11 Encryption Protocols

Sandesh Jain, Sarthak Pruthi, Vivek Yadav

Department of Information Technology
Delhi Technological University, Delhi,India

Abstract - **The widespread usage of smart terminals such as smartphones, which provide significant convenience in our daily lives, has resulted in an increase in information security issues. Researchers are increasingly concerned about network security and calculations. As more devices join a wireless network, important and sensitive data is transferred over the air between users, making data packets easy to sniff and grab. The purpose of this project is to perform penetration testing to find flaws in the WEP, WPA, and 802.11i WPA2, WPA3 security protocols, as well as to conduct anonymous attacks against them using the macchanger script. Penetration testing in WEP was carried out using Kali Linux and its Aircrack-ng tools, which exploited a 4-way handshake for WPA/WPA2.**

Index Terms— **Encryption, Protocols, WPA, WPA2, four-way handshake, KRACK, WPA3.**

I. INTRODUCTION

Wireless networks are one of the more recent innovations that the internet has brought into our lives. Wireless technology is the mechanism of sharing information using invisible waves in the air using electromagnetic or acoustic waves. The challenge of information security is becoming increasingly critical as wireless network technology develops and gets more widely used.

Wireless Fidelity (WiFi) is a modern wireless network model defined by the IEEE 802.11 standard. A hostile activity intended targeting wireless system information or wireless networks is known as a wireless attack. The wireless network has several faults of its own. It uses radio waves to send signals and must first establish a connection before being used. A penetration test is a malicious attack on a target system that achieves access control by emulating an attacker's techniques and methods with the client's legal authorization; it is a test method for evaluating information system security control measures. This paper provides a WiFi penetration test method based on Kali Linux that uses methods such as monitoring, sniffing, capturing, data analysis, WiFi password cracking, pseudo-wireless access point spoofing, and other techniques to improve the security of WiFi networks.

II. LITERATURE REVIEW

In most residential and business networks, the IEEE 802.11 standard defines WLAN characteristics; 802 deals with LAN and MAN, while.11 deals with WLAN. The available radio frequency spectrum varies significantly depending on the regulatory domain. Collision-avoidance carrier-sense multiple access and medium access control are used in the 802.11 protocol family, which means that equipment listens for other users on a channel before transmitting each frame. The first edition of the standard was released in 1997. The protocols are typically used in conjunction with IEEE 802.2 to carry Internet Protocol traffic. 802.11a, 802.11b, and 802.11g are the most extensively used and supported standards.

III. TOOLS AND TECHNOLOGIES USED

Tools and Technologies used to implement and perform working model to wifi encryption were:

- Wifi Adapter
- Raspberry pi kit
- Wifi Router
- Raspberry Pi (Power Adapter)
- Bluetooth Adapter
- Kali Linux
- Aircrack-ng, Airodump-ng, Airplay-ng

IV. WLAN PROTOCOLS

A. Working on WLAN Protocols

1. Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy(WEP) is a security protocol which was introduced as part of IEEE 802.11 standard in 1997. It uses an RC4 encryption algorithm to encrypt the plain text and unencrypted integrity check value to ensure the integrity of the plain text when it is transmitted from one end to the other. It operates at the data link layer and the physical layer. In 2001 major flaws such as short IV size, keystream reuse which proved that data transmitted can be easily captured and

tampered. With these flaws WPA was introduced to remove the vulnerability of weak encryption techniques.

2. Wireless Protected Access(WPA)

WPA was created as a WiFi security protocol. It's similar to WEP, but it encrypts data using a temporal key integrity technique (TKIP). To avoid the attacks that WEP allows, TKIP provides a new 128-bit key for each packet. Users can upgrade to TKIP from earlier WLAN equipment without changing hardware because TKIP comprises several methods that encapsulate WEP. Message integrity Check (MIC), IV sequencing mechanism, Per-packet key mixing function, and Re-keying mechanism are four additional algorithms included in TKIP to boost key strength.

A per-packet key mixing mechanism is used to improve cryptographic strength. A re-keying approach is employed to generate a new key for every 10,000 packets. A hashing-based initialization-vector sequencing technique is used. WPA uses TKIP, which dynamically changes the encryption key used by the computers, preventing intruders from matching the secure network's encryption key. A message authentication code (MAC) is a cryptographic way of confirming that communications have not been tampered with. WPA uses the Extensible Authentication Protocol (EAP) to authenticate computers rather than relying exclusively on the plaintext of their MAC address.

3. Wireless Protected Access2(WPA2)

Although Wi-Fi signals are broadcast in the air and can be readily intercepted, encrypting wireless data is critical for security. WPA II is an 802.11 wireless security standard that employs 128-bit encryption and passwords to prevent unauthorized access to critical information.

This protocol uses a single pass-key (PSK) that all devices and the Access Point share for network authentication. The PSK can be 8 to 63 characters long. An attacker can gain access to the network if he discovers this one-of-a-kind PSK. Every device develops and maintains a PMK based on the PSK or the AP name until it changes. When a client attempts to connect to an authenticator, the 4-way handshake procedure begins, and a Pairwise Transient Key (PTK) is generated, which is used to encrypt data between a client and an access point and is changed at least once every 65,535 packets.

Pairwise Master Key Generation

Using the function below, all devices calculate PMK from PSK. The data is encoded using HMAC-SHA1 by the key derivation function PBKDF2. These routines are used to reduce vulnerabilities to brute force attacks because of their high computational cost.

PMK = PBKDF2(HMAC-SHA1, PSK, SSID, 4096, 256)

B. Comparison of Different WLAN Protocols

	WEP	WPA	WPA2	WPA3
RELEASE YEAR	1999	2003	2004	2018
ENCRYPTION METHOD	Rivest Cipher 4(RC4)	Temporal Key Integrity Protocol(TKIP) with RC4	CCMP and Advanced Encryption Standard	Advanced Encryption Standard (AES)
SESSION KEY SIZE	40-bit	128-bit	128-bit	128-bit(Personal) 192-bit(Enterprise)
CIPHER TYPE	Stream	Stream	Block	Block
DATA INTEGRITY	CRC-32	Message Integrity Code	CBC-MAC	Secure Hash Algorithm
KEY MANAGEMENT	NA	4-Way handshaking mechanism	4-Way handshaking mechanism	Simultaneous Authentication
AUTHENTICATION	WPE-Open WPE-shared	Pre-Shared Key	Pre-Shared Key	Simultaneous Authentication of equals with EAP variant

C. Vulnerability/Weaknesses of WLAN Protocols

1. Vulnerability of WEP

As IV is short i.e of 24 bits, there can be cases when two packets are captured using the same IV. This shows the vulnerability of Short IV size. Also as there is no particular way to generate IV, there can be a possibility when wifi is using the same IV for a long period of time. This highlights the Keystream vulnerability. When plain text is associated with the unencrypted Integrity Check Value , it leads to brute force attacks by the attackers.

2. Vulnerability of WPA/WPA2-PSK

WPA is similar to WEP, but it uses temporal key integrity protocol(TKIP) to increase the encryption. TKIP encapsulates WEP using various algorithms. WPA2 on the other hand uses Advanced Encryption Standard. Communication of packets between the Client and Authenticator occurs using a 4-way handshake and it takes place between client and AP whenever a client tries to connect to an AP. PMK is calculated using the PBKDF2 hashing technique. By entering SSID, self-created

pass, and SSID length into this method, the attacker can build a hashed key and compare it to the captured hashed key. The AP and client verify that the credentials (WPA Key) used to initiate the connection are correct and then exchange the key to encrypt all the traffic from that point onwards.

The cryptographic key is installed whenever the client receives the third handshake message. A 4-way handshake's weak point lies at this stage, where messages might be misplaced or deleted. When the AP fails to receive message 4 (acknowledgement message) from the client, it re-transmits message 3 and lets the client receive it several times by reinstalling the same cryptographic key each time the third message is received. The assault takes place here.

3. Vulnerability of WPA3

WPA3 shows vulnerability in its DragonFly Handshake where dragonfly means the mechanism through which the user authenticates itself. It uses strong elliptical curves for encryption but hackers can force it to use weaker curves for encryption.Another vulnerability is side channel attack which uses an unprotected code, i.e which can be modified using if-then-else branch in Dragonfly algorithm to guess the password generation method.

D. Attacks on WLAN protocols

1. Attack on WEP

One can capture the packet and inject it into traffic to force an access point for creating a new packet with a new IV and continue to do so till there are two packets using the same IV. Using the vulnerability of short IV size one can figure out the secret key used in encrypting and decrypting the plain text.

1.1 Sniff all packets from target Access Point using the command - **"*airodump-ng --channel 2 --bssid <MAC ADDRESS> --write packets wlan0*".**

It will capture all packets and store them in .cap file format.

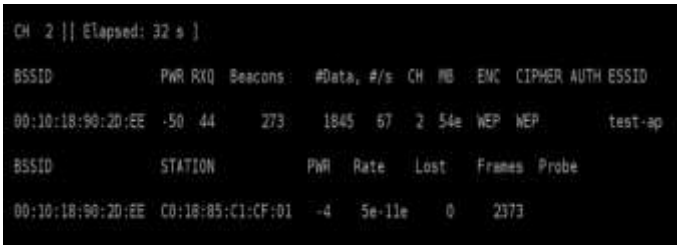

Figure 1. Sniff all the packets from the target AP

1.2 Crack WEP Key from the captured packets using the command - *"**aircrack-ng <filename of stored packets>**".*

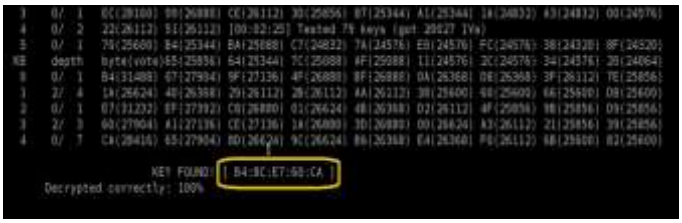

Figure 2. Cracking WEP key from the captured packets

2. Attack on WPA/WPA2

2.1 PTK is generated using PMK and PBKDF2 hashing function, this is the loophole for attackers to exploit as this data is sent in an unencrypted format. The pass, which can be computed via a dictionary attack with a solid 4-way handshake captured, is the attacker's lone unknown value in computing the PMK. We don't have a cryptographic flaw in WPA2, thus there's no other method to reverse engineer that key.

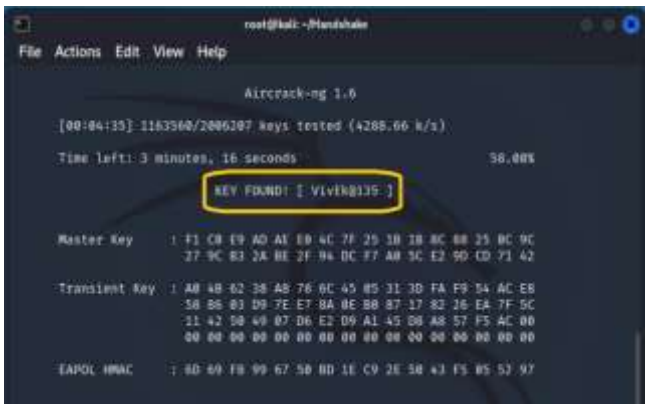

Fig 3. Cracking passphrase from the captured four-way handshake

2.3 KRACK for WPA2 (Key Reinstallation Attack)
It's used to get around the WPA2 protocol's weakness. As previously mentioned, the attacker can impersonate the AP by re-transmitting message-3 multiple times. When the client attempts to reconnect to the AP, the attacker can force it to connect to the phoney AP. It can operate as a middleman. Attackers can crack the pass with the captured handshake using brute force and dictionary assaults.

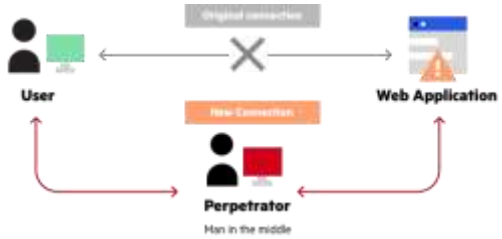

Fig 4. Cracking passphrase using KRACK

3. Attack on WPA3

Downgrade Attack - As some devices do not support new protocols, transition mode can be exploited through two different ways. First one is to modify the beacons by being man in the middle showing that a WPA3-enabled router can only be used as WPA2. And second is if the SSID name of the targeted WPA3 network is known, one can forge a man in the middle redirecting every request of WPA3 to connect to WPA2 access point. Once it act as WPA2 attacker can exploit the four way handshake of WPA2 above as explained in attacks of WPA2

E. MAC SPOOFING

For protecting the individual's privacy, mac address should be anonymous. **Therefore MAC SPOOFING is done before performing any kind of attack on the above mentioned protocols.**

Algorithm to spoof MAC address:

1 ifconfig wlan0 down (Down the interface)
2 macchanger -a wlan0 (Change the mac address)
3 ifconfig wlan0 up (Up the interface)

Store this code in the crontab so that whenever the system starts code execute itself and mac address get changed automatically.

Figure 5: Mac Spoofing Script

Pseudo-Code to spoof MAC address using macchanger.

```
Create a bash script using nano (filename).sh
Write the following command
    ifconfig (interface) down
    macchanger -A (interface)
    ifconfig (interface) up
Execute it using ./filename.sh
For changing MAC address every time you reboot, use the
crontab -e command as every time you reboot the system, a
command written in crontab gets executed.
Write the following in crontab:
    "@reboot /root/filename.sh"
```

Fig 6. Pseudo Code for MacChanger

VI. CONCLUSION

WEP was introduced in 1999 it has a vulnerability of short IV size which leads to cracking of WEP key. WPA was introduced in 2003 which uses TKIP that dynamically changes the key which system uses. In the case of WEP the key was static. Later on in 2004 WPA2 was introduced to mitigate the chances of brute force attacks which was seen in WPA by using Advanced Encryption Standard techniques. As key in WPA2 can be cracked using KRACK attack, later on in 2018 WPA3 protocol was introduced which has a different and longer key size as compared to the other protocols. Also WPA3 uses a simultaneous authentication method. Still some downgrade attacks can be performed on WPA3 as described above. Every protocol has some vulnerabilities which lead to cracking of password for different wifi. These are getting mitigated as soon as they are identified.

VII. REFERENCES

[1] G. Ola, "Penetration Testing on a Wireless Network .," 2013.

[2] A. O. Karen Scarfone, Murugiah Souppaya, Amanda Cody, "Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology," *Nist Spec. Publ.*, vol. 800, pp. 1–80, 2008, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800.

[3] M. Vanhoef and F. Piessens, "Key Reinstallation Attacks," pp. 1313–1328, 2017, doi: 10.1145/3133956.3134027.

[4] N. Golmie, N. Chevrollier, and O. Rebala, "Bluetooth and WLAN coexistence: challenges and solutions," *IEEE Wirel. Commun.*, vol. 10, no. 6, pp. 22–29, Dec. 2003, doi: 10.1109/MWC.2003.1265849.

[5] M. Kyei and M. Asante, "Penetration Testing of IEEE 802.11 Encryption Protocols using Kali Linux Hacking Tools," *Int. J. Comput. Appl.*, vol. 176, no. 32, pp. 26–33, 2020, doi: 10.5120/ijca2020920365.

[6] T. Kropeit, "Don't Trust Open Hotspots: Wi-Fi Hacker Detection and Privacy Protection via Smartphone," 2015.

[7] A. Yacchirena, D. Alulema, D. Aguilar, D. Morocho, F. Encalada, and E. Granizo, "Analysis of attack and protection systems in Wi-Fi wireless networks under the Linux operating system," in *2016 IEEE International Conference on Automatica (ICA-ACCA)*, Oct. 2016, pp. 1–7, doi: 10.1109/ICA-ACCA.2016.7778423.

[8] H. Peng, "WIFI network information security analysis research," in *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, Apr. 2012, pp. 2243–2245, doi: 10.1109/CECNet.2012.6201786.

[9] Y. Chen, W. Wang, and Q. Zhang, "Privacy-preserving location authentication in WiFi with fine-grained physical layer information," in *2014 IEEE Global Communications Conference*, Dec. 2014, pp. 4827–4832, doi: 10.1109/GLOCOM.2014.7037570.

[10] A. Ye, Q. Li, Q. Zhang, and B. Cheng, "Detection of Spoofing Attacks in WLAN-Based Positioning Systems Using WiFi Hotspot Tags," *IEEE Access*, vol. 8, no. 1, pp. 39768–39780, 2020, doi: 10.1109/ACCESS.2020.2976189.

[11] S. Dhall, S. K. Pal, and K. Sharma, "A chaos-based probabilistic block cipher for image encryption," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 1, pp. 1533–1543, Jan. 2022, doi: 10.1016/j.jksuci.2018.09.015.

[12] D. Kumar and D. S. S., "Enhancing Security Mechanisms for Healthcare Informatics Using Ubiquitous Cloud," *J. Ubiquitous Comput. Commun. Technol.*, vol. 2, no. 1, pp. 19–28, 2020, doi: 10.36548/jucct.2020.1.003.

[13] S. Shakya, "an Efficient Security Framework for Data Migration in a Cloud Computing Environment," *J. Artif. Intell. Capsul. Networks*, vol. 01, no. 01, pp. 45–53, 2019, doi: 10.36548/jaicn.2019.1.006.

[14] P. W. Nätverk, "PUBLIC WI-FI NETWORKS Sammanfattning."

[15] S. Sukhija and S. Gupta, "Wireless Network Security Protocols A Comparative Study," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 2, no. 1, 2012.

AUTHORS

First Author – Sandesh Jain, Department of Information Technology, Delhi Technological University, Delhi,India, sandeshjain_2k18it109@dtu.ac.in

Second Author – Sarthak Pruthi, Department of Information Technology, Delhi Technological University, Delhi,India, sarthakpruthi_2k18it110@dtu.ac.in

Third Author – Vivek Yadav, Department of Information Technology, Delhi Technological University, Delhi,India, vivekyadav_2k18it131@dtu.ac.in

Correspondence Author – Dr. Kapil Sharma, Head of Department of Information Technology, Delhi Technological University, Delhi,India, kapil@ieee.org