International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May-2018 www.irjet.net p-ISSN: 2395-0072

Mitigation of Key Reinstallation Attack in WPA2 Wi-Fi networks by detection of Nonce Reuse

Prof. Naitik S.T[1], Raiton Lobo[2], Pradnya Shyam Vernekar[3], Vamshi G Shetty[4]

[1]Professor, Dept. of Information Science and Engineering, Sahyadri College of Engineering and Management, *Adyar, Karnataka, India,*

[2,3,4]*Student, Dept. of Information Science and Engineering, Sahyadri College of Engineering and Management , Adyar, Karnataka, India.*

Abstract - *Serious weaknesses were discovered in WPA2, a protocol that secures all modern protected Wi-Fi networks. An attacker within range of a victim can exploit these weaknesses using key reinstallation attacks (KRACKs). Concretely, attackers can use this novel attack technique to read information that was previously assumed to be safely encrypted. This can be abused to steal sensitive information such as credit card numbers, passwords, chat messages, emails, photos, and so on. The attack works against all modern protected WPA2- Wi-Fi networks. Depending on the handshake mechanism, it is also possible to inject and manipulate data. A solution is proposed to provide the secure handshake by capturing and analyzing the EAPOL packets to prevent nonce reuse which happens while reinstallation of Pairwise Trasient Key (PTK) which happens in case if there is an attack. Our patches blocks access to the victim system via rogue AP created by the KRACK and alerts the client about the suspicious activity and blocks the attacker from further attacking.*

Key Words: reinstallation, nonce, rogue AP, handshake, WPA2 (Minimum 5 to 8 key words)…

1. INTRODUCTION

Network security has policies and practices done so that it can monitor and remove unauthorized access for the data, and changing, misuse of data or denial of a computer network. Network security will allow us to have the access to data in a network which is authorized. The Network Administrator will control all these data. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network and data security should be a high priority when considering a network operation due to the growing threats of hackers trying to infect the network. For enterprises, security is important to prevent them from potential business loss. Wireless Fidelity (Wi-Fi) is the wireless networking technology, which provides wireless connection for internet with high-speed using radio waves. It uses radio frequency technology between the sender and the receiver but does not have any physical wired connection between them. The radio frequency is a frequency associated with radio wave propagation in the electromagnetic spectrum. We can protect the Wi-Fi networks by using Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP). The strongest is the WPA2 which is used to protect the Wi-Fi network from the hackers. WEP's improved version is WPA and WPA2 for better security of Wi-Fi. By upgrading of firmware on wireless network interface cards we can implement WPA. For WPA, Temporal Key Integrity Protocol (TKIP) was adopted. TKIP continuously generates a new 128-bit key for each packet that is it has per-packet key and because of this it prevents the type of attack that are done on WEP. WPA also consist of Message Integrity Check. In this, altering and resending data packets are not allowed to be done by attacker. WPA2 is most commonly used security protocol to authenticate and protect Wi-Fi networks for both enterprise and personal settings worldwide. Using key reinstallation attacks, an attacker within range of a victim can exploit these weaknesses. By using this method, attackers can read information that was previously assumed to be safely encrypted. This can be abused to steal sensitive information such as credit card numbers, passwords, chat messages, emails, photos, and so on. The attack works against all modern protected Wi-Fi networks. Depending on the network configuration, it is also possible to inject and manipulate data. For example, an attacker might be able to inject ransomware or other malware into websites.

2. LITERATURE REVIEW

The IEEE 802.11i standard has been analyzed and a DoS attack has been identified. They have used Isabelle tool to analyze the 4-way handshake phase and it also identifies a new Denial-of-Service (DOS) attack and it has been used to implement the linear temporal logic framework. The selective DoS attack prevents the authenticator from receiving message 4 after the supplicant sends it. The DOS attack forces the authenticator to re-send the message 3 until timeout and subsequently to de-authenticate supplicant by sending de authenticating packets [1].

Two improved mechanism were provided: (1)They encrypted A Nonce and in this method they avoided transmission of plaintext of ANonce and enhanced the security of message1. (2) Message1 integrity detection method is the method used for Message Integrity Check(MIC) verification of message 1. And it finally analyzes the security of improvement mechanism [2].

A novel, highly practical, and targeted variant of a wireless evil twin attack against WPA Enterprise networks is presented in this paper. The practical importance of the Weak binding between wireless network SSIDs and authentication server certificates are highlighted in this paper. A prototype implementation of the attack, its effectiveness and cost and countermeasures that should be adopted are described. The experiments demonstrate that, with 17 technically-sophisticated users show that the attack is stealthy and effective in practice [3].

It describes a man-in-the-middle attack on protocol like HTTP authentication inside a TLS tunnel. If tunnelled and untunnelled forms are used in legacy client authentication protocol there is the possibility of it being vulnerable. It results to insecure system even if both the client authentication protocol and the tunnel protocol are both kept secure [4].

Wi-Fi network preparation in production system uses intrusion detection systems Snort and Kismet; to evaluate whether the system is under attack or not. The response reaction of IDSs is monitored using Penetration Testing which uses Backtrack 5 R3 with Fern Wi-Fi Cracker and Ettercap. In order to find the response characteristics of Snort and Kismet, the description of attack is done. And Wireshark is used by the system to analyze the result After the attack is completed in terms of the captured traffic [5].

The usage of Wireshark as a packet sniffer is shown to perform the penetration testing of websites. This method of information gathering technique is used to indicate whether a website is secure or vulnerable [6].

3. PROBLEM STATEMENT

Proposing solution for the detection and blocking of reuse of nonces in the 4-way handshake mechanism of WPA-2 Wi-Fi based networks.

4. ARCHITECTURE DIAGRAM

Architecture diagram consists of components such as Client device, Attacker, Router and Wireless local area network which is used for connection that is protected by WPA2 protocol and the internet.

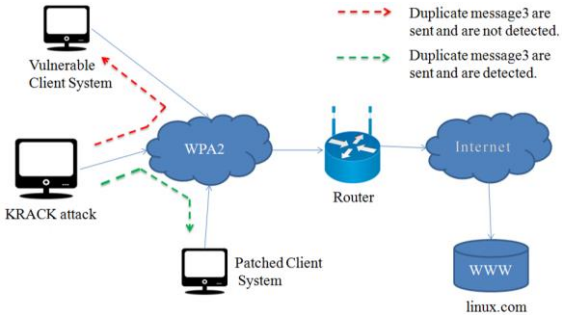

Fig -1: Architecture Diagram for Solution for KRACK Attack

All Wi-Fi networks which are protected by WPA2 use the 4-way handshake mechanism to generate a fresh session key. This handshake has was even proven secure for a long time. The the 4-way handshake mechanism takes place between the client and the wireless access point which is actually the exchange of four messages between them. The attacker obtains a channel-based man in the middle position between the client device and the access point. The attacker blocks the fourth message which arrives at the authenticator from the client device. This causes the third message to be arriving repeatedly at the client device which causes the session key to be reinstalled. When this happens, the associated parameters of the session key which are the nonce and the replay counter are reset to their initial values. Depending on the security protocol used, this allows an adversary to replay, decrypt, and/or forge packets.

5. Methodology

5.1. Attack

1. Disable Wi-Fi in network manager

2. Remove unused virtual interfaces to start from a clean state

3. Configure monitor mode on interfaces

4. Open the patched hostapd instance that carries out tests and let it start

5. Let scapy handle DHCP requests

6. Close hostapd and clean up

7. Configure gateway IP: reply to ARP and ping requests

8. for client in set-of-clients

9. Test the 4-way handshake

10. Manipulate Handshake messages

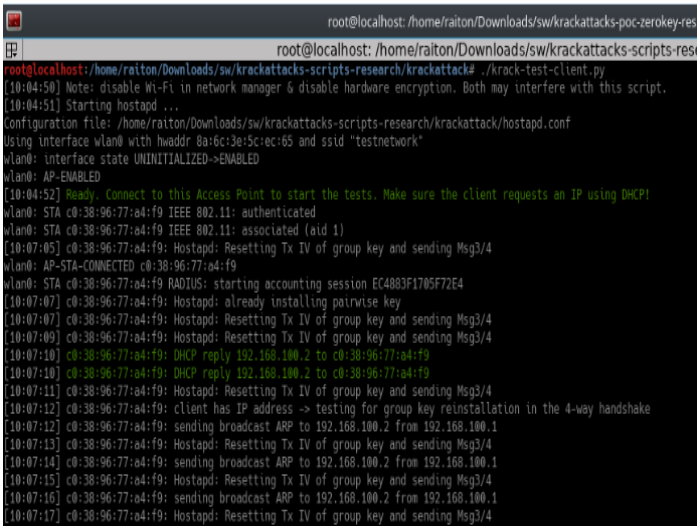

Fig -2: Creation of Rogue AP in the Attacker System

Here, we first disable the Wi-Fi in network manager to avoid the conflict with the script. We then remove the virtual unused interfaces if they may be active. Then we configure the monitor mode which enables a device with a wireless network interface controller to sniff all traffic received from the wireless network. We then open the patched instance of hostapd which was created while installing the scripts and we let scapy to handle DHCP requests. Then we test the client for the variant of the attack to which it seems vulnerable after which we manipulate its handshake messages.

5.2 Internet Forwarding

1. Get Wireless Interface
2. Configuring IP address of malicious AP
3. Enable IP forwarding
4. Enable NAT
5. Enable SSLStrip rerouting
6. Start DHCP and DNS service

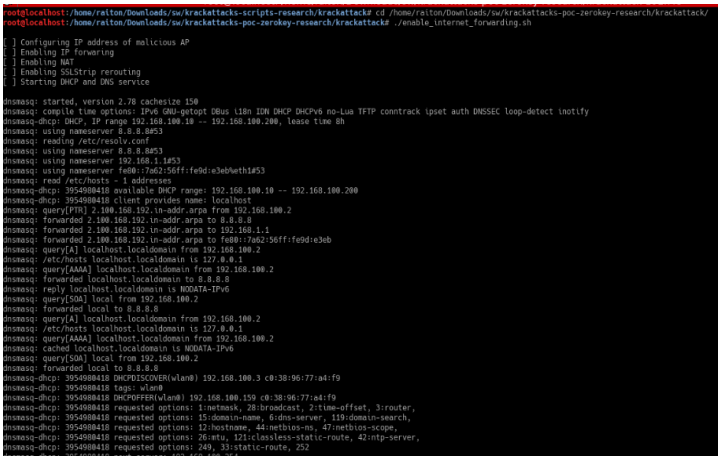

Fig -3: Forwarding Internet through the Attacker System

This is used to forward the internet to the victim system. It first obtains the wireless interface. On the server computer, static IPv4 address is assigned to the interface connected to the other machines. Then we enable NAT using iptables and SSLStrip rerouting. Then, DHCP and DNS service is started.

5.3 Solution

1. Get Wireless Interface
2. Monitor the Wireless Interface
3. Create a network socket
4. Receive data from the socket
5. Extract Ethernet layer
6. Extract IEEE802.1x header
7. Extract WPA key data
8. Check for duplicate EAPOL packet message 3
9. Disconnect the Attack

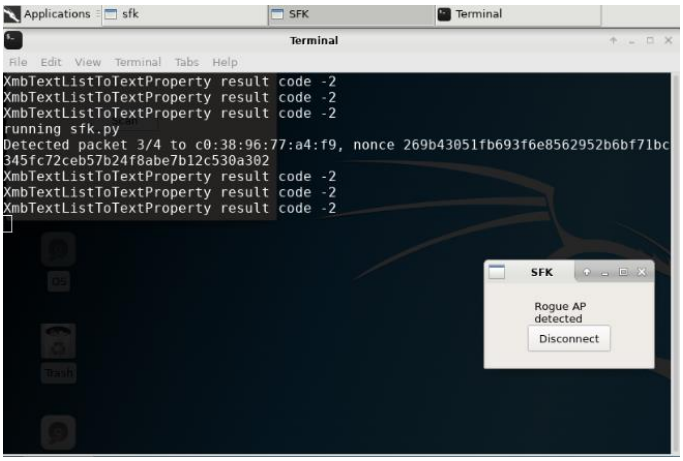

Fig -4: Detection of Rogue AP

Here, we first get the Wireless Interface of the device and monitor the traffic owing through the device. Network socket is created and data is received from the socket. Ethernet layer is extracted from which IEEE802.1x header is extracted. WPA key data is extracted from the IEEE802.1x header and we get the position of the nonce using it. Then we check for duplicate message 3 from EAPOL packet using the reuse of the nonces. Then the victim is alerted if there is a possible KRACK attacks.

6. RESULT AND ANALYSIS

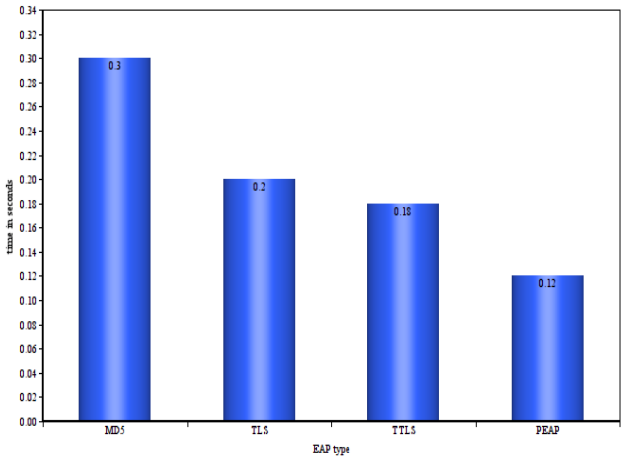

Chart -1: Variation of Time with respect to EAPOL packets

This graph shows the variation of time with respect to different types of EAPOL packets. Time in milliseconds is plotted in x-axis and the types of EAPOL packets is plotted in y-axis.

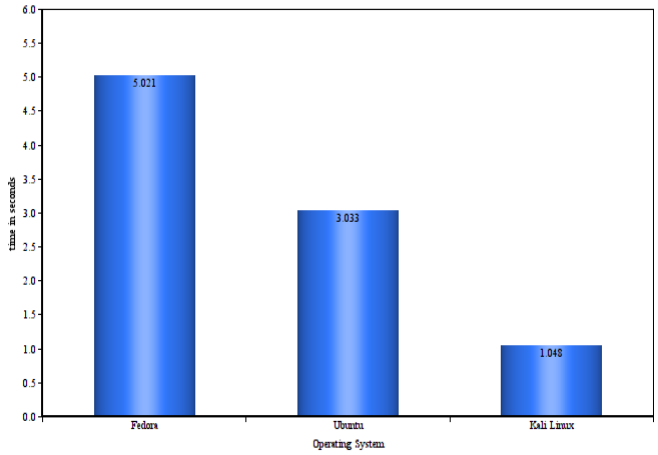

Chart -2: Variation of Time of Detection in different Operating Systems

This graph shows the variation of time with respect to different types of Operating Systems. Time in milliseconds is plotted in x-axis and the types of Operating Systems.

6. CONCLUSIONS

The technique to detect and prevent the KRACK attack is demonstrated. The authentication of client using WPA2 Wi-Fi AP is done by 4-way handshake mechanism. During authentication we have detected the nonce reuse by observing the transmission of message3 twice. Hence we developed a solution for KRACK attack by disconnecting the victim from rogue AP and alerting the victim by sending message that the rogue AP is detected. In this technique we analyze about the authentication process of WPA2 Wi-Fi networks. Our solution is able to prevent the user from becoming victim of KRACK attack.

As a future enhancement the detection of KRACK attack could be explored in Windows & IOS platforms to make the wifi a secure networking environment for testing and get services.

REFERENCES

[1] Abdullah Alabdulatif, Xiaoqi May, Lars Nolle, "Analyzing and attacking the 4-way handshake of IEEE 802.11i standard", 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013): 382 – 387, 2013.

[2] Senbai Dalabaev, Sun Quanfu, Li Qinghua, "4-way handshake attack analysis and improvement in 802.11i", 2013 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference: 455 - 458, 2013.

[3] Aldo Cassola and William Robertson, "A Practical, Targeted, and Stealthy Attack Against WPA Enterprise Authentication", Northeastern University College of Computer and Information Science.

[4] N. Asokan, Valtteri Niemi, Kaisa Nyberg, "Man-in-the-Middle in Tunneled Authentication Protocols", Nokia Research Center, Finland. November 11, 2002.

[5] Ana Yacchirena, Darwin Alulema , Darwin Aguilar, "Analysis of attack and protection systems in Wi-Fi wireless networks under the Linux operating system", 2016 IEEE International Conference on Automatica (ICA-ACCA): 1 – 7 , 2016.

[6] S. Sandhya and Sohini Purkayastha, "Assessment of website security by penetration testing using Wireshark", 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS): 1 - 4, 2017.