Defenseless Victims of WiFi Hack- A Model Based on Fluxion

* Ms. N. Ashwini,
Ph.D. Research Fellow, Reg. No. 19214012042058, Department of Criminology and Criminal Justice,
Manonmaniam Sundaranar University, Tirunelveli

**Dr. Syed Umarhathab,
Assistant Professor, Department of Criminology and Criminal Justice, Manonmaniam Sundaranar
University, Tirunelveli

ABSTRACT

Wireless Local Area Networks a significant part of the time implied as WLANs or Wi-Fi frameworks are all the energy of late. People are presenting these in houses, establishments, work environments and motels, etc, with no vain. Searching for fulfilling the remote solicitations, Wi-Fi item merchants and administration givers are exploding up as quick as would be judicious. Remote systems offer handiness, compactness, and can even be more reasonable to attempt than wired frameworks. With the customer request, merchant arrangements and industry benchmarks, remote system innovation is exact and is delving in for the long stretch. In any case, how far this development is going give a verified circumstance to the extent security remains a strange issue. Understanding the various dangers and vulnerabilities related with 802.11-based remote systems and morally hacking them to make them increasingly secure is the thing that this paper is all about. On this fragment, we'll hold onto a gander at normal dangers, vulnerabilities related with remote systems. Also, besides we have analyzed the entire strategy of WiFi, centering the need to get comfortable with apparatuses like Cain, NetStumbler, Kismet, MiniStumbler and fluxion (Evil twin attack) to help the model/study the territory and tests we should run to fortify our air flags and point by point outline of our own usage will follow lastly, there will be a segment on the best way to secure oneself against this sort of cyber attack which is one of emerging forms of cyber crimes.

***Keywords* -** WiFi Hacking; WEP; Kismet; Cain; NetStumbler, Fluxion

I . INTRODUCTION

Today mobile devices are all around us and are now affecting everything we doing everyday life would be a somewhat minor statement to make, however constant growth in this popular area of technology can mean that it is sometimes efficient. If we think what's been going on and what will be the impact. If we jump back a trivial 10-12 years, we would be placed in an era where the majority of computers were still wired to a network with a trusty old Ethernet cable, and mobile phones were simply handy devices for making phone calls, playing snake and sending text messages are there. But according to the fast forward days we have powerful computers that can carry easily in our pockets boasting quad core processors and wireless network cards, some of the vehicles like cars that can connect to Wi-Fi, 3G and 4G networks, and tablets that will take care of most of our everyday work and respite needs. With more and more organizations or societies adopting these devices every day it got thinking to us about how secure such devices can be because we all travel with our mobile devices, carry them everywhere with us where we use to travels most–By their very nature mobile devices present a number of immediate and interesting properties such as knowing which Wi-Fi networks they are connecting to when you are out? How accessible is the stored data once it has been stolen? What happens if the tool is misplaced or stolen? But during recent years, Wireless networks are becoming very popular due to its wide range users can connect it via their mobile phone (smart- phones), laptops, tablets etc. They can connect to WiFi connections called “hotspot”inpublic as well as private area only difference is of security, you need wifi password before connecting at private places but there is an open connection to all the users at public places, no security or password is required, so the chances of fraud are more which is referred toas “Evil Twin Attack”. Public places are like Airports, Hotels, Shopping points such as complex or malls etc. There are some of the advantages of Wi-Fi such as people can stay online all the time or Wi-Fi also provide high speed, unlimited downloading or surfing’s or some provide limited data like data-packs in mobile phones.

II. NEED TO TEST OUR WIRELESS ARRANGEMENTS

Weakness of Wireless systems is on track as far back as the untimely days of the 802.ll b standard of 1990s. The standard's introduction, major 802.11 restrictions, for example, physical security, encryption imperfections has been discovered. Because of these, two remote security principles have turned out to enable battle to back at the enemy:

Wi-Fi Protected Access (WPA) : Developed by the Wi-Fi Alliance, filled in as an interceding standard to settle the outstanding WEP vulnerabilities.

IEEE 802.l1i (recognized as WPA2) : An authority IEEE standard, that coordinate the WP A fixes for WEP with extra encryption and confirmation mechanisms. Like numerous security measures, the issue with these remote security arrangements isn't that they don't work, this is a result of the system executives who are impervious to change and don't completely actualize them. They don't prefer to reconfigure their remote frameworks and would prefer not to actualize new security components feeling that the administration winds up troublesome. These look like insignificant things, however they withdraw numerous remote systems exposed and holding up to be traded off. In spite of the fact that WPA, WPA2 and the different remote assurance strategies depicted in this paper have been executed, system may in any case be in danger. As up to our training, we have seen numerous giving some security systems either the over ones or the other. However, even with numerous remote security gauges and endor arrangements accessible, the larger parts of frameworks are still completely open to ambush.

III. SECURITY CONCERNS OF WI-FI SYSTEMS

Wi-fi systems are broadly utilized today. Surely, it is difficult to envision being in a city and not having a Wi-fi hotspot inside 100 yards. Notwithstanding, regardless of the way that they are so normal and simple to use, Wi-fi systems show a scope of security Vulnerabilities. Some of those are because of blemished convention outline, and some are because of client botches, however as a rule it is a mix of both. We show some of these security worries here:

- Some Wi-fi systems are absolutely unprotected, as in they give no encryption of the information exchanged through the system. In any case, those cases are relatively obsessive these days as a large portion of the Wi-fi systems do in fact utilize a type of security/encryption.
- Even if some sort of encryption is utilized, it might be low security and in this manner effectively pliant. Take for instance the convention WEP(Wired Equivalent Privacy). It used the RC4 figure, which is a stream figure. It is fundamental, for such ciphers, that the key is constantly revived, in the event that we need to guarantee secrecy. With a specific end goal to accomplish this, the convention utilized an IV of 24 bits.
- Even when a solid encryption convention is used, it is conceivable to utilize parcel sniffers, for example, Wireshark, keeping in mind the end goal to screen the movement that experiences the system.

IV. ASSESSING FOR PROTECTION

Once in the event that we get everything adapted, it's an ideal opportunity to make our sleeves and uncover our hands messy via completing unique moral hacks against our wireless set-up. There are bunch of security tests we can perform to know how weak our remote frameworks are to trouble. The results of these tests will definitely demonstrate to us what security punctures may or may not be settled to construct a more secure wireless network.. We will draw out different balance measures we can utilize to settle the shortcomings we recognize. In the next few segments,, we will layout an assortment of security assaults to build up the pull for weakness tests we'll be working against our wireless network.

A. Exploitative Attacks

These sorts of assaults exploit human shortcomings like absence of cognizance, carelessness and disregarding outsiders. We likewise encase physical vulnerabilities which can influence an intruder to have a possibility on firsthand access to our wireless gadgets. These assaults consolidate,

- Flouting into wireless gadgets that customers mounted on their own and left unsecured
- Some kind of assaults where a programmer phony as some person else and induce clients to give out unnecessarily much data about our system
- Unauthorized evaluation of APs, radio wires and a few different remote foundation to reconfigure and confine information off it.

B. Assaults Concerning Network

There are a gathering of procedures the critical folks can use to break inside our remote domain or at any rate abandon it shriveled in a nonworking state. System based assaults involve,

- Mounting fiendishness wireless APs and avoiding remote customers into connecting to them.
- Holding information off the system from a separation by under our own steam and so forth.
- Attacking the exchanges of the customer in arrange by sending up MAC addresses, setting up a medium (Opening in a remote framework in the middle of an AP and remote client) and the sky is the limit from there
- Abusing system conventions
- Carrying Denial-of-benefit (DoS) assaults
- Jamming RF signals

C. Assaults Concerning Software

Since the security hurts with the 802.11 convention weren't sufficient, we must be restless about working frameworks and utilities on wireless customer machines promptly helpless against misuse. Presently we'll a portion of the product assaults:

- Hacking the working framework and further applications on remote customer equip
- Contravening through default settings like passwords also, SSIDs that are easily known
- Cracking WEP keys and pattering into the system's encryption conspire
- Getting route in by the utilization of weak system validation techniques

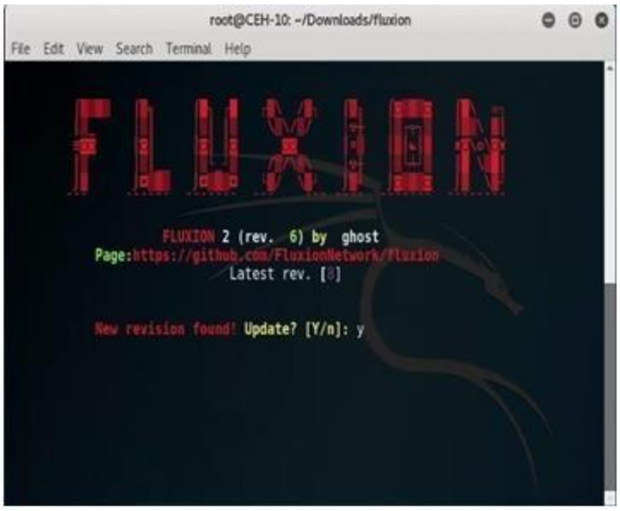
V. SIMPLE HACK WITH A FLUXION

Fluxion is a unique tool in its use of a WPA handshake to not only control the behavior of the login page, but the behavior of the entire script. It jams the original network and creates a clone with the same name, enticing the disconnected user to join. This presents a fake login page indicating the router needs to restart or load firmware and requests the network password to proceed. fluxion is the future-a blend of technical and social engineering automation that trick a user into handing over the Wi-Fi password in a matter of keystrokes. Specifically, it's a social engineering framework using an evil twin access point (AP), integrated jamming, and handshake capture functions to ignore hardware and focus on the "wetware."

IMPLEMENTATION FLUXION TOOL:

To get Fluxion running on our Kali Linux system, clone the git repository with: git clone https://github.com/wi-fi-analyzer/fluxion & then Run the Fluxion command again with sudo

./fluxion to get hacking below In figure 1

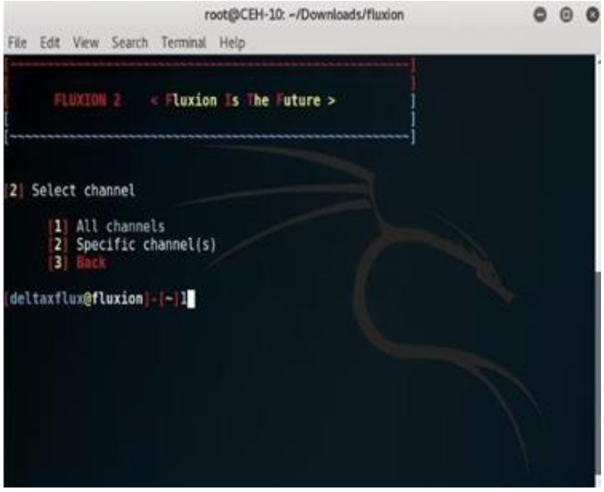


root@CEH-10: ~/Downloads/fluxion
File Edit View Search Terminal Help

```
FLUXION

          FLUXION 2 (rev.  6) by  ghost
    Page:https://github.com/FluxionNetwork/fluxion
                     Latest rev. [8]


    New revision found! Update? [Y/n]: y
```

Figure 1 : Fluxion configuration

In below figure 2,the first option is to select the language. Select your language by typing the number next to it and press enter to proceed to the target identification stage. Then, if the channel of the network you wish to attack is known, you may enter 2 to narrow the scan to the desired channel. Otherwise, select 1 to scan all channels and allow the scan to collect wireless data for at least 20 seconds Select a target with active clients for the attack to run on by entering the number next to it.

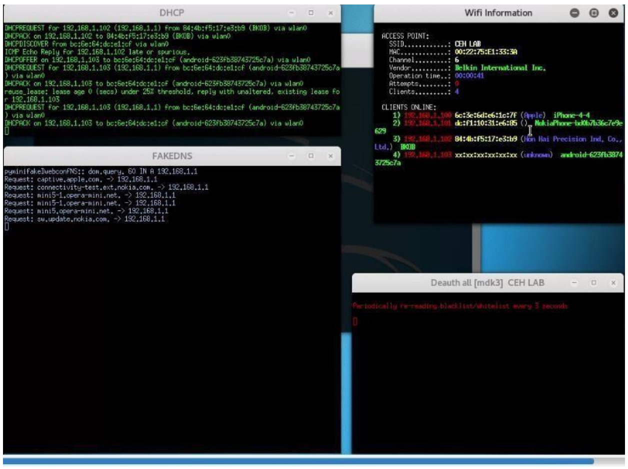


root@CEH-10: ~/Downloads/fluxion
File Edit View Search Terminal Help

```
[-----------------------------------------------------]
[                                                     ]
[     FLUXION 2    < Fluxion Is The Future >          ]
[                                                     ]
[-----------------------------------------------------]


[2] Select channel

     [1] All channels
     [2] Specific channel(s)
     [3] Back

[deltaxflux@fluxion]-[~] 1
```

Figure 2: Scan your Wi-Fi Ap target

Using the Aircrack-ng method by selecting option 1 ("aircrack-ng"), Fluxion will send deauthentication packets to the target AP as the client and listen in on the resulting WPA handshake. When you see the handshake appear, as it does in the top right of the screenshot below, you have captured the handshake. Type 1 (for "Check handshake") and enter to load the handshake into our attack configuration below figure 3 Once you've typed the number of the target network, press enter to load the network profile into the attack selector. For our purpose, we will use option 1 to make a "FakeAP" using Hostapd. This will create a fake hotspot using the captured information to clone the target access point. Type 1 and press enter and above figure 5 gathered the wifi information on AP.



```
DHCPREQUEST for 192.168.1.102 (192.168.1.1) from 84:4b:f5:17:e3:b9 (BKOB) via wlan0
DHCPACK on 192.168.1.102 to 84:4b:f5:17:e3:b9 (BKOB) via wlan0
DHCPDISCOVER from bc:6e:64:dc:e1:cf via wlan0
ICMP Echo Reply for 192.168.1.102 late or spurious.
DHCPOFFER on 192.168.1.103 to bc:6e:64:dc:e1:cf (android-623fb38743725c7a) via wlan0
DHCPREQUEST for 192.168.1.103 (192.168.1.1) from bc:6e:64:dc:e1:cf (android-623fb38743725c7a
) via wlan0
DHCPACK on 192.168.1.103 to bc:6e:64:dc:e1:cf (android-623fb38743725c7a) via wlan0
reuse_lease: lease age 0 (secs) under 25% threshold, reply with unaltered, existing lease fo
r 192.168.1.103
DHCPREQUEST for 192.168.1.103 (192.168.1.1) from bc:6e:64:dc:e1:cf (android-623fb38743725c7a
) via wlan0
DHCPACK on 192.168.1.103 to bc:6e:64:dc:e1:cf (android-623fb38743725c7a) via wlan0
```

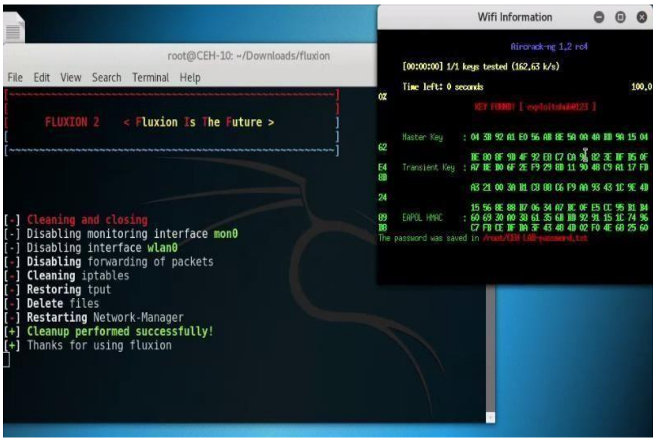
```
pyminifakeDwebconfNS:: dom.query. 60 IN A 192.168.1.1
Request: captive.apple.com. -> 192.168.1.1
Request: connectivity-test.ext.nokia.com. -> 192.168.1.1
Request: mini5-1.opera-mini.net. -> 192.168.1.1
Request: mini5-1.opera-mini.net. -> 192.168.1.1
Request: mini5.opera-mini.net. -> 192.168.1.1
Request: sw.update.nokia.com. -> 192.168.1.1
```

```
 ACCESS POINT:
   SSID............: CEH LAB
   MAC.............: 00:22:75:E1:33:3A
   Channel.........: 6
   Vendor..........: Belkin International Inc.
   Operation time..: 00:00:41
   Attempts........: 0
   Clients.........: 4

 CLIENTS ONLINE:
     1) 192.168.1.100 6c:3e:6d:e6:1c:7f (Apple)  iPhone-4-4
     2) 192.168.1.101 dc:f1:10:31:e6:85 ()  NokiaPhone-bd0b7b36c7e9e
629
     3) 192.168.1.102 84:4b:f5:17:e3:b9 (Hon Hai Precision Ind. Co.,
Ltd.)  BKOB
     4) 192.168.1.103 xx:xx:xx:xx:xx:xx (unknown)  android-623fb3874
3725c7a
```

```
Periodically re-reading blacklist/whitelist every 3 seconds
```

Figure 3 : FakeAP which fluxion

In below figure 6 , The user is directed to a fake login page, which is either convincing or not, depending on which you choose.


root@CEH-10: ~/Downloads/fluxion
File Edit View Search Terminal Help
Wifi Information

```
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]
[                                                                  ]
[      FLUXION 2    < Fluxion Is The Future >                      ]
[                                                                  ]
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]


[-] Cleaning and closing
[-] Disabling monitoring interface mon0
[-] Disabling interface wlan0
[-] Disabling forwarding of packets
[-] Cleaning iptables
[-] Restoring tput
[-] Delete files
[-] Restarting Network-Manager
[+] Cleanup performed successfully!
[+] Thanks for using fluxion
```

```
                          Aircrack-ng 1.2 rc4

      [00:00:00] 1/1 keys tested (162.63 k/s)

      Time left: 0 seconds                                  100.0
0%
                      KEY FOUND! [ [illegible] ]


      Master Key     : 04 3B 92 A1 E0 56 A8 8E 5A 0A 4A BD 9A 15 04
62
                       BE 80 0F 9D 4F 92 EB C7 CA 9A 82 3E DF D5 0F
E4    Transient Key  : A7 BE B0 6F 2E F9 29 8D 11 90 48 C9 A1 17 FD
8D
                       A3 21 00 3A D1 C8 08 C6 F9 AA 93 43 1C 9E 4D
24
                       15 56 8E 88 B7 06 34 A7 BC 0F E5 CC 95 B1 B4
09    EAPOL HMAC     : 60 69 30 A0 38 61 35 6B DD 92 91 15 1C 74 96
D8                     C7 FB CE DF DA 3F 43 48 4D 02 F0 4E 68 25 60
The password was saved in /root/CEH LAB-password.txt
```

Figure 6 : Capture the password using fluxion

Entering the wrong password will fail the handshake verification, and the user is prompted to try again. Upon entering the correct password, Aircrack-ng verifies and saves the password to a text file while displaying it on the screen. The user is directed to a "thank you" screen as the jamming ceases and the fake access point shuts down.

Vulnerability :

Evil twin attacks happens in various forms, but the vulnerability many times come from humans. This include vendors such as an airport, coffee shop, or book store which provide its customers free wifi access without any network encryption password (WEP or WPA).This for the most part originates from the inconvenience of building up the pre-sharing secret word. Evil- twin attacks also exploit the common desires of general public who want to access free wifi. Therefore, an attacker with a machine capable of broadcasting wifi signal can establish himself as a legit AP on the premise and trick the user to connect to it.

Prevention :

There are no absolute tool/mechanism to totally take out evil twin assault. Following are a few recommendations for relief

- Configure the remote settings of the OS to interface just to favored systems and just upon demands.
- Avoid interfacing with unreliable systems and perusing delicate/individual data, for example, managing an account.
- Use outside programming, for example, Air Personal to warn user of unusual wireless activity.

VI. CONCLUSION

Wireless Networks like Wi-Fi being the most spread innovation over the world is vulnerable to the threats of Hacking.. It is critical to shield a network from the hackers in order to prevent exploitation of confidential data. The better way to do this is, just think like a hacker. At a glance, we've discussed the entire procedure of splitting WEP encryption of Wi-Fi in this paper. All this is made only to figure out the necessity in getting touch with some of the scanning tools like NetStumbler, Cain, Kismet, MiniStumbler, Fluxion and so forth to review the Wireless region. The tools that have been expressed will offer us the capacity to reprieve our claim WEP key and this might be an ideal opportunity to go to the following rank of security, the WPA. Give us a chance to endeavor to hack all the gauges of Wireless systems morally with a specific end goal to make a framework extremely secured.

REFERENCES

[1] L. Zhou and ZJ. Haas, "Securing Ad Hoc Networks," IEEE Network, vol. 13, no. 6, 1999, pp. 24-30.

[2] Jinyang Li, Charles Blake, Douglas S. J. De Couto, Hu Imm Lee, Robert Morris, "Capacity of Ad Hoc

Wireless Networks," In Proc. of Mobicom (mobicomOl) conference, 200l.

[3] M. Junaid , Dr Muid Mufti, M.Umar Ilyas, "Vulnerabilities of IEEE S02.11i Wireless LAN," Transactions On Engineering, Computing And Technology Vll February 2006 Issn 1305-5313.

[4] Martin Beck, Erik Tews, "Practical attacks against WEP and WPA," November S, 200S.

[5] US-CERT, "Using Wireless Technology Securely," produced by USCERT, a government organization, 200S.

[6] Michael Roche, "Wireless Hacking Tools, "available at http://www.cse.wustl.edul-jain/cse571-07/ftp/wireless_hacking

[7] R. Terarnura, Y. Asakura, T. Ohigashi, H. Kuwakado, and M. Morii, "Breaking WEP with Any 104-bit Keys - All WEP Keys Can Be Recovered Using IP Packets Only," Proc. of SCIS2009, CDROM, 1A2-6, Jan. 2009.

[8] Jeremy Martin, "The art of casual WiFi Hacking," CISSP-ISSAP, 2009.

[9] D. Waterman (Eds.), "Interconnection and the internet': Selected papers from the 1996 TC conference.

[10] V. Moen, H. Raddum, and KJ. Hole, "Weaknesses in the temporal key hash of WPA," ACM SIGMOBILE Mobile Computing and Communications Review, vol.S, pp.76-S3, 2004.

[11] Stanley, Richard A."Wireless LAN risks and vulnerabilities," Information systems control Journal, volume2, 2002.

[12] Wireless Ethernet Compatibility Alliance, http://www.wirelessethernet.org/index.htrnl

[13] WiFi -Windows, http://www.oxid.it (Cain & Able) http://www.NetStumbler.com

[14] Regina D Hartley, "Ethical Hacking: Teaching Students To Hack"

[15] Wiley Publications, "Introduction To Ethical Hacking," available at www.media.wiley.com

[16] https://null byte.wonderhowto.com/how-to/hack- wi-fi-capturing-wpa-passwords-by-targeting-users- with- fluxion-attack-0176134/