Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 11805 - 11812
Received 25 April 2021; Accepted 08 May 2021.

Wireless Security – An Introduction to Wireless Security Protocols and their Security Flaws

[1]Alakshendra Sharma, [2]Tushar Bhatia, [2]Avijit Katyar, Samson Ebenezar U[4]
[1 2 3 4] Department of Computing Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India
[1] salakshendra@gmail.com, [2]15tushar.bhatia@gmail.com,
[3]avijitktr295@gmail.com,[4] u.ebenezar@galgotiasuniversity.edu.in

Abstract

As we are moving forward with technology ,the Internet is becoming an important part of our life. We want to be connected to the internet at every second of our lives. As all of the countries are now trying to give free wifi at public places at a high speed. Common people do not know how it can be dangerous to connect to a public wifi. So as to increase the data security of the user communicating on a public wifi, there are some security protocols which are being constantly updated to give the best user experience and data privacy. In this research paper we are going to introduce you to the various protocols and wireless communication standards that were previously used for security purposes and what were the security flaws in those protocols with a demonstration of why we should use the latest wireless security protocol and will conclude by summarizing the security vulnerability in various protocols.

Keywords
Internet;Protocols,Security,Privacy

Introduction

The Internet is becoming an important part of people's lives because of the WFH situation all around the world. It is now the most important thing for people to stay connected to the internet 24/7 .Wireless networks help us to work and connect to the internet without being physically present in the organization. Security of data in wireless networks is as important as having access to the internet .There are various Standards , security protocols which help in moving data from one network to another with Confidentiality and Integrity . As all security standards are not fully secured and since the last part of the 1990s, Wi-Fi security conventions have gone through various updates, with out and out censure of more seasoned conventions and critical modification to more up to date conventions. A walk around the historical backdrop of Wi-Fi security serves to feature both what's out there at the present moment and why you ought to dodge more seasoned norms. Now we will look at one of the first security protocols which helped in securely authenticating a user on a wireless network..

Literature Review

In the new years we have a colossal advancement of remote innovation. We are as of now getting more subject to remote innovation. As we probably are aware remote organizations

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 11805 - 11812
Received 25 April 2021; Accepted 08 May 2021.

have communicated nature so there are diverse security issues in the remote correspondence. The security shows proposed for the wired frameworks can't be extrapolated to remote frameworks. Programmers and interlopers can make use of the provisions of remote correspondence.

In this paper we will consider the distinctive far off security threats to remote frameworks and shows currently open like Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). WPA2 is a more generous security show as contrasted with WPA in light of the fact that it uses the Advanced Encryption Standard (AES) encryption. There are not many issues in WPA2 like it is defenceless against beast power assault and MIC pieces could be used by developers to contrast it and the decoded content. So, in this paper we will focus on various kinds of remote security risks.

TOOLS USED –

1. Kali Linux - A Penetration Testing distro which has a lot of tools to crack Wifi Authentication
2. Airmon-ng – A Tool which help in putting the wireless card in monitor mode without authenticating
3. Airodump-ng – To capture raw packets of all the nearby networks.
4. Aircrack-ng – Tools for brute forcing the key

Hardware Required –

1. Any wifi external card with a good range coverage and which can support monitor mode

WEP

Introduction to WEP

Wired Equivalent Privacy (WEP) is a security convention, indicated in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b, that is intended to give a remote neighborhood (WLAN) with a degree of security and protection practically identical to what in particular is typically expected of a wired LAN. A wired neighborhood (LAN) is for the most part ensured by actual security instruments (controlled admittance to a structure, for instance) that are powerful for a controlled actual climate, however might be ineffectual for WLANs since radio waves are not really limited by the dividers containing the organization. WEP tries to build up comparable insurance to that offered by the wired organization's actual safety efforts by scrambling information sent over the WLAN. Information encryption secures the weak remote connection among customers and passageways; when this measure has been taken, other commonplace LAN security components like secret word assurance, start to finish encryption, virtual private organizations (VPNs), and validation can be set up to guarantee protection.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 11805 - 11812
Received 25 April 2021; Accepted 08 May 2021.

Working of WEP

WEP utilizes the RC4 calculation to scramble the parcels of data as they are conveyed from the passageway or remote organization card. When the passage gets the parcels sent by the client's organization card it decodes them. Every byte of information will be scrambled utilizing an alternate bundle key. This guarantees that if a programmer figures out how to break this parcel key the solitary data that is spilled is what is contained in that bundle. The genuine encryption rationale in RC4 is extremely basic. The plain content is XOR-ed with a vastly long key stream. The security of RC4 comes from the mystery of the bundle key that is obtained from the key stream.

Cracking WEP Authentication

It is very easy to crack WEP Authentication with various tools present in the penetration distro like kali Linux parrot os, Arch Linux, Black-Box..Steps to crack WEP are as follows:

1. Put the wireless Card in Monitor Mode using Airmon-ng , this tool helps to sniff packet

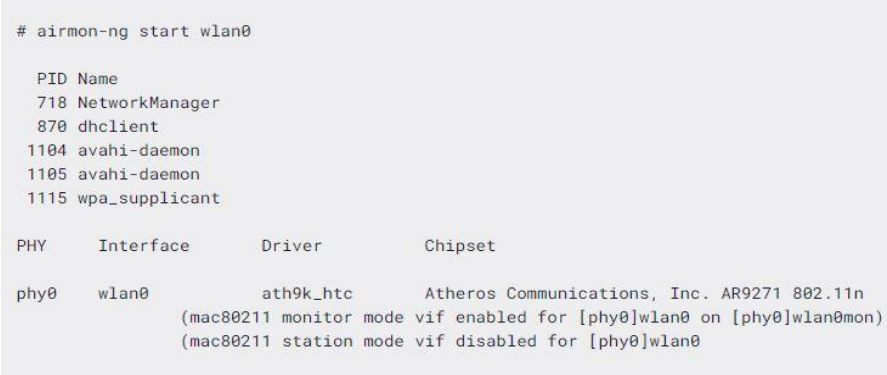

Figure1. Wireless Card In Monitor Mode

2. Now we have to Use Airodump-ng to capture packet in their raw form .It is a utility which help us in capturing 3-way handshake which in turn will help in cracking the key .The Airodump-ng captures the packet , bssid etc and creates a capture file with all the packets stored in it.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 11805 - 11812
Received 25 April 2021; Accepted 08 May 2021.

```
# airodump-ng
CH  9 ][ Elapsed: 1 min ][ 2007-04-26 17:41 ][ WPA handshake: 00:14:6C:7E:40:80

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 00:09:5B:1C:AA:1D   11  16       10        0    0  11  54.  OPN              NETGEAR
 00:14:6C:7A:41:81   34 100       57       14    1   9  11e  WEP  WEP         bigbear
 00:14:6C:7E:40:80   32 100      752       73    2   9  54   WPA  TKIP   PSK  teddy

 BSSID              STATION            PWR   Rate   Lost  Packets  Notes  Probes

 00:14:6C:7A:41:81  00:0F:B5:32:31:31   51   36-24    2       14
 (not associated)   00:14:A4:3F:8D:13   19    0-0     0        4           mossy
 00:14:6C:7A:41:81  00:0C:41:52:D1:D1   -1   36-36    0        5
 00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2   35   54-54    0       99           teddy
```

Figure2. Capturing Of Packets

3. After capturing a significant amount of packets , we can supply this packet to the tool Aircrack-ng, Aircrack-ng is a solid tool to crack wifi password because it uses statistical ,bruteforce and dictionary attack to crack the pass phrase.

```
Aircrack-ng 1.4

                [00:00:03] 230 keys tested (73.41 k/s)

                        KEY FOUND! [ biscotte ]

    Master Key     : CD D7 9A 5A CF B0 70 C7 E9 D1 02 3B 87 02 85 D6
                     39 E4 30 B3 2F 31 AA 37 AC 82 5A 55 B5 55 24 EE

    Transcient Key : 33 55 0B FC 4F 24 84 F4 9A 38 B3 D0 89 83 D2 49
                     73 F9 DE 89 67 A6 6D 2B 8E 46 2C 07 47 6A CE 08
                     AD FB 65 D6 13 A9 9F 2C 65 E4 A6 08 F2 5A 67 97
                     D9 6F 76 5B 8C D3 DF 13 2F BC DA 6A 6E D9 62 CD

    EAPOL HMAC     : 52 27 B8 3F 73 7C 45 A0 05 97 69 5C 30 78 60 BD
```

Figure3. Cracked WiFi Password

Note: We have to capture enough packets to capture a three-way handshake in order to crack the password .

As we can see, the authentication password of a WEP secured network can be easily cracked using the above tools . One of the few ways to not let that happen is by using lengthy and uncommon passwords ..A password with a length of 8 to 15 characters with special characters and numeric , upper case , lower case is much harder to crack using any of the traditional methods of cracking .

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 11805 - 11812
Received 25 April 2021; Accepted 08 May 2021.

Disadvantage of using WEP

1. WEP's first shortcoming is the clear mathematical constraint of the 24-bit Initialization Vector (IV), which brings about 16,777,216 (224) potential qualities. This may appear to be enormous, however you know from conversations in Chapter 4, "Security Protocols," that this number is misleading. The issue with this modest number is that in the end the qualities and hence the keys begin rehashing themselves; this is the manner by which aggressors can break the WEP key

2. The subsequent shortcoming is that of the conceivable 16 million qualities, not every one of them are acceptable. For instance, the number 1 would not be excellent. On the off chance that an aggressor can utilize an instrument to locate the feeble IV qualities, the WEP can be broken

3. WEP's third shortcoming is the distinction between the 64-bit and 128-bit encryption. Discernment would show that the 128-cycle ought to be twice as secure, correct? Wrong. The two levels actually utilize a similar 24-digit IV, which has innate shortcomings. Thus, in the event that you think going to 128-cycles is safer, in actuality, you will definitely acquire no increment in the security of your organization.

WPA2

Introduction to WPA2

Wifi Protected Access or commonly known as WPA2 is a security feature added to WPA for wireless networks that provides robust data protection and network access control. WPA2 ensures that a high level of protection is provided in the wireless network and only authorized persons can access the network and the data transmitted over the network. WPA2- Personal and Wpa2-Enterprise are the two versions of WPA. WPA2-Personal prevents unauthorized access to the network by setting up a password for the network. WPA2-Enterprise checks for the authorized user through the server.

Working of WPA2

WPA2 uses CCMP which is a new AES based encryption technique for more security. WPA2 is based on IEEE 802.11i standards. WPA2 mainly uses the Advanced Encryption Standard (AES) algorithm for the encryption of the network traffic. WPA2 uses a key size of 128 bits for the encryption of data. The AES Encryption process in WPA2 is done either by AES or by using TKIP (Temporal Key Integrity Protocol).
WPA2 creates secure communication in four phases. The first phase being authentication and pre authentication method .In this phase AP and the client will agree on security policy. In the second phase a master key will be generated. In the third phase temporal keys will be created in a regular manner. In phase four, all keys generated in phase three will be used by CCMP protocol to provide data integrity and data confidentiality.
WPA2 is immune to most types of network attacks like Man in the middle attack, Brute Force attack, dictionary attack .WPA2 is based on Robust Security Network (RSN) which helps in achieving all the features provided by WPA along with extra features for security.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 11805 - 11812
Received 25 April 2021; Accepted 08 May 2021.

WPA2 supports authentication for both infrastructure and ad hoc networks whereas WPA supports Infrastructure Network.

Attacking a WPA Secured Network

Attacking a WPA secured network is not that simple, we have capture more packets than WEP and capturing a 3-way handshake is not that simple.

2.Putting the wireless card in monitor mode.

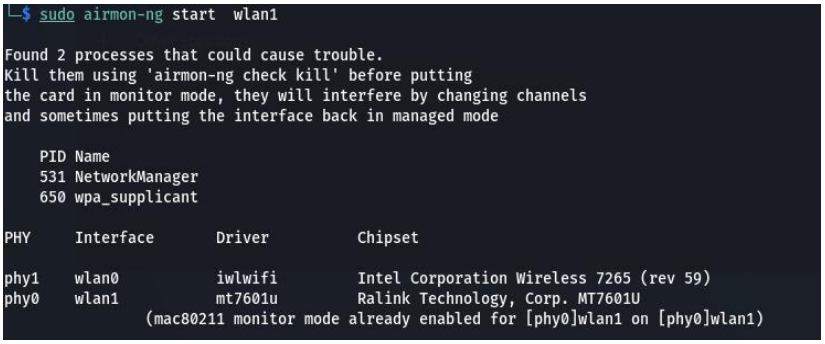

Figure4. Putting wireless card in monitor mode

2.Capturing the packets of WPA network

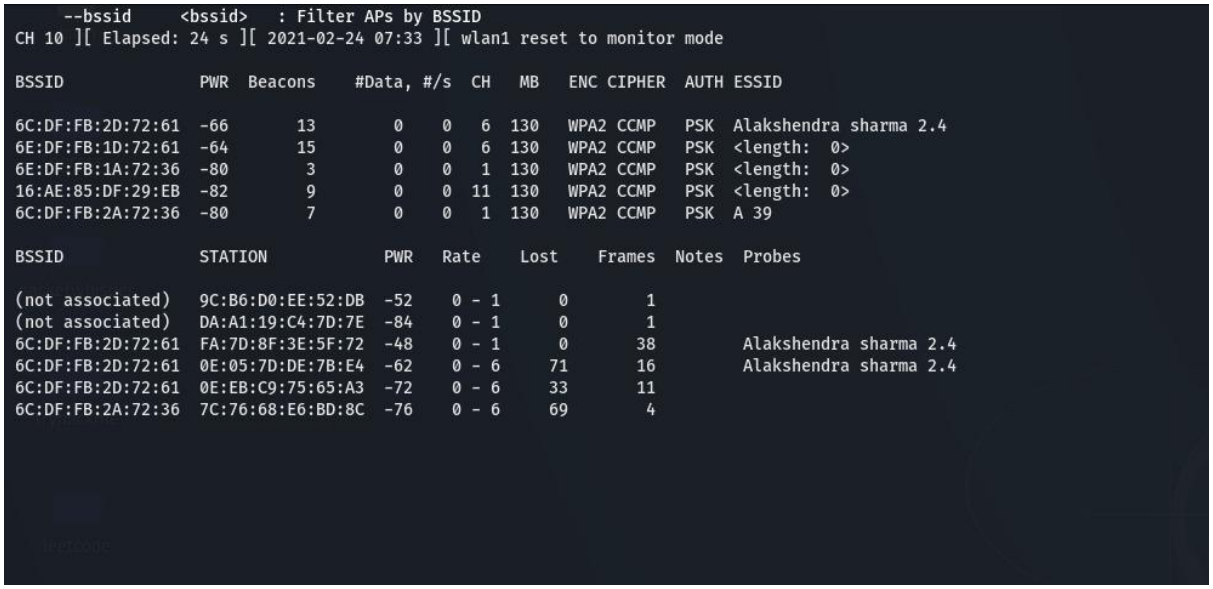

Figure5. Capturing The Packets

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 11805 - 11812
Received 25 April 2021; Accepted 08 May 2021.

3.Cracking the passphrase using Aircrack-ng

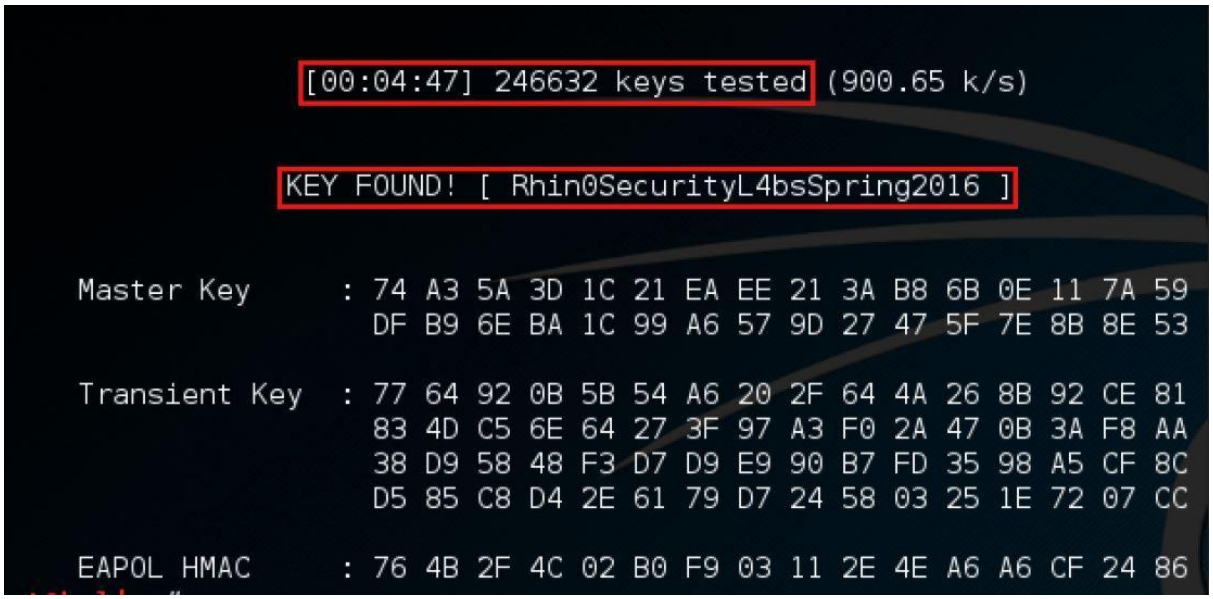

Figure 6. Cracked WiFi Password

WPA2 Advantages

WPA utilizes a lot more grounded encryption calculations than its archetype. WPA utilizes a Temporary Key Integrity Protocol (TKIP), which progressively changes the key as information bundles are sent across the organization. Since the key is continually transforming, it makes breaking the key substantially more troublesome than that of WEP. On the off chance that the need emerges to change the worldwide key, WPA will naturally promote the new key to all gadgets in the organization without having to physically transform them.

Disadvantages

Weaknesses to utilizing WPA are not many, with the greatest issue being incongruence with heritage equipment and more seasoned working frameworks. WPA likewise has a bigger exhibition overhead and builds information parcel size prompting longer transmission.

WPA 3

Introduction to WPA3

WPA3 is the next generation of Wi-Fi security. All devices powered by WPA3 use the latest security measures, do not allow expired asset policies, and require the use of protected frames (PMF). However, devices with WPA3 are not yet readily available.
There are other improvements involved in WPA3. This is OWE (Optional Wireless Encryption). OWE is a technology designed for Social Networks. With this technology, automatic encryption will be performed without user intervention. Think about this. You are at Starbucks and working with your PC. With WPA2, any attacker in the same community area as you, can make Man-in-the-Middle attacks target your system. They can start a Dictionary Attack for your password. With WPA3, it is blocked.
WPA2 is vulnerable to dictionary attacks that are used to predict passwords with many different attempts. Hackers can do this even if they are not on the same network as the victim.

To prevent this type of attack, WPA3 offers a new Key Exchange Protocol. With this protocol, it will use a secure method, One-Time Equal Authentication. Previously, with WPA2, the Hand way handshake was used and this is at risk.
WPA3 offers more security and encryption compared to WPA2. With WPA3, all the road between you and the other limit will be encrypted, until the other limit is verified.
There is also a new type of connection to come with WPA3. With this new version, you can use QR Codes to connect devices to networks. For example, you can use your smartphone to scan QR Code of Printers, Access Points etc. and then connect to the entry point, printer or any other device that will be in our lives via Internet of Things (IoT). This type of communication will require additional security. Therefore, WPA3 is a good solution for this.

Conclusion

At last, after analyzing all the main wireless security protocols we can say that each of them had done their work successfully in their time, but as technology started to grow and new hardware and software came in , the attack surface increased for the hackers to target wireless security protocols in a whole new way . From above situation we have learn that, it is most important to time to time upgrade of the protocols according to the need.
As more people are getting on the internet, it is most important to provide a secure path to the user to access the internet with proper security and data privacy .

References

1. https://www.brighthub.com/computing/smb-security/articles/78216/
2. https://rhinosecuritylabs.com/penetration-testing/wpa-hacking-introduction-wifi-network-security/
3. Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3) Dr. B. Indira Reddy, V. Srikanth
4. https://www.aircrack-ng.org/doku.php?id=simple_wep_crack
5. https://www.networkworld.com/article/3316567/what-is-wpa3-wi-fi-security-protocol-strengthens-connections.html
6. WIRELESS SECURITY AND THREATS Muhammad Imran Tariq
7. https://www.aircrack-ng.org/doku.php?id=simple_wep_crack
8. https://www.aircrack-ng.org/doku.php?id=airmon-ng
9. https://null-byte.wonderhowto.com/how-to/wi-fi-hacking/
10. A Study of Wireless Network Security Ningwei Sun *Governors State University*