National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Cyber Encryption

A. Sruthi
The Kingdom College, Bengaluru, Karnataka, India

ABSTRACT

The paper talks about the introduction of wireless security, modes of unauthorized access and security measures. I intend to explain the generation of protocols used and their pros and cons. I also define the encryption keys that were used in each generation to manipulate security. Finally I conclude with certain protocols and their combinations that are more secured in this generation.

Keywords : Encryption, protocols and combinations.

I. INTRODUCTION

At present everyone wants to access internet; for this, people are connecting their smart phones, laptops, computers and other devices with wireless network. For example a Business man wants to transact by connecting to the wireless network or an employee of a company wants to share a document with other branch employee.

Globally for every purpose people are using Wi-Fi network so that their tasks are completed in fraction of seconds. But for any invention we do have advantages and disadvantages. While using Wi-Fi networks people have to secure their data and systems. So I am here to explain Wi-Fi security.

Wireless Security means safeguarding the devices like smart phones, computers, laptops and other devices along withthe networks they are connected to from unapproved access.

Wi-Fi is becoming very popular since last decade. We can observe Wi-Fi in airports, malls, libraries, coffee shops, hotels, and other public venues etc…

A wireless network uses radio waves to transmit data instead of wired connections.There are 4 environments built around wireless technology, they are:

1. Hardware or Software based Access Point.
2. Multiple Access Point.
3. LAN-to-LAN wireless network. 4.3G and 4G hot spot.

Modes of unauthorized Access:

Accidental association
When a user wants to connect with a wireless network, the user looks out for a nearby network which has a strong network. Later the user connects his device to that particular network. If that network is under the surveillance of the attacker, then the user data is hacked. So Accidental association is nothing but without the knowledge of the user their devices are surveillanced by hackers.
Malicious association

This happens when a wireless device wants to connect with laptops known as “soft APs”. These laptops are created when a cyber criminal runs his software that makes the wireless network card look like a legal access point. Once the criminal gets access,

they can easily steal passwords, launch attacks or plant viruses to the network.

Ad hoc networks

Ad hoc networks are defined as peer-to-peer networks. Actually there is no internet connection, attackers setup these kind of networks and make them visible like an actual internet connection with a name Free Wi-Fi. When a user connects to the Ad hoc network they are revealing their devices to attack.

Non-traditional networks

Usually people mainly concentrate on laptops and Access points to be secured. Non-traditional networks focuses on PDA's, printers etc…, through these devices cyber criminals are injecting the threats to wireless networks.

Identity theft (MAC spoofing)

Every NIC(Network Interface Card) provides a connection to a router which contains a unique MAC (Media Access Control) address. By using this facility we have filters called MAC filtering to allow certain addresses into the network. If an attacker is listening to a network traffic and gets the MAC address of any computer,it can be very useful to an attacker. The attacker uses this MAC address and enters into the secured networks this is called

MAC spoofing(stealing and using the MAC address). Man-in-the-middle attacks.

This attack is similar to malicious association. An attacker tempts devices to sign into a computer called "soft AP", if the user connects his devices with this computer the attacker connects to the real Access Point through some NIC.

Denial of service

This attacks usually makes the network traffic slow down or cause the network to crash. The Denial of service attacks are meant to disturb the network services. So that legal networks may be unable to connect or use the network.

Caffe Latte attack

In the past, if a hacker wants to attack a network; they had to be in the range of wireless network but by this Caffe Latte attack he could not be in the range to attack the network. This attack is to retrieve WEP encryption key.

Secured Protocols used in wireless security:

1) Wired Equivalent Privacy(WEP):

It was developed in 1999; a64 bit WEP uses 40 bit encryption key concatenated with a 24-bit initialization vector(IV) to form the Rivest Cipher 4(RC4) key and which was easily hacked by unauthorized users. To increase more security later we introduced a 104 bit(concatenated with 24 bit totally 128 bits), 128 bit (combined with 24 bit totally 152 bits), 232 bit(combined with 24 bits of system generated data i.e., totally 256 bits).Even though we could make it secure, effortlessly hackers could discover the WEP key. So that this protocol is not used at present and even the modern Wi-Fi routers don't have the option of WEP. To achieve more security WPA was introduced.

2) Wi-Fi Protected Access(WPA):

The new version of security protocol called WPA was developed in the year 2003 to solve the problems of WEP. It is far better than WEP, began implementation of IEEE 802.11i Standard, it uses a stronger encryption method called TKIP (Temporary Key Integrity Protocol). TKIP dynamically changes its keys for each data packet. When TKIP encryption used, MIC (Message Integrity Code) is included to check the data is not hacked is known as Cyclic Redundancy Checking(CRC).

This is the major improvement in WPA compared with WEP.

3) Wi-Fi Protected Access II (WPA2):

WPA with TKIP could only be capable of encrypting "short" i.e., 128 bytes data packets. This leads TKIP to be substituted with CCMP also named as AES-CCMP (Advanced Encryption Standard- Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) encryption protocol.WPA2 was developed to provide even stronger security than WPS. Which is available from the year 2004.

The list of Wi-Fi security protocols available on the routers are:

1. WPA2+AES
2. WPA+AES
3. WPA+TKIP/AES
4. WPA+TKIP
5. WEP

6) Open Network (no security)

The order is from more security to less security and the last option is without security which means we are not setting up any key for the network so that any visitor can easily enter into that network. We can find these kind of networks in public places like Theaters, Hotels, and Resorts etc…
4) Wi-Fi Protected Access III (WPA3):
WPA3 was introduced in 2018, it adds new features to simplify Wi-Fi

Solutions:

minutes the user has to press the button on the printer to connect to the network.
2. WPS Pin number method: Like the WPS push method, the user has to enter the WPS pin number in the box and within few seconds it will connect to the printer security and enable more authentication. WPA3 upgrades to 128 bit encryption and uses SAE(Simultaneous Authentication of Equals) which is known as Dragonfly Handshake.
5) Wi-Fi Protected Setup (WPS): Designed for people who know about wirCeless networks to make it as easy as possible for devices to join a secure wireless network. In this setupwe have two methods of which either of them can be used.

1. WPS Push method:
Most routers today have physical WPS button and a lot of Wi-Fi supported printers have WPS button. If the user presses WPS button on the router, within 2

1. Change default Administrator
Username and passwords.
2. Change the default SSID(Service Set Identifier) name and hide the same.
3. Use a strong password and use good wireless encryption.
4. Turn off guest network and turn on device lists to view the devices which are connected to your Wi-Fi so that we can block the unsafe devices.
5. Enable MAC (Media Access Control) address filtering.

II. CONCLUSION

Globally people are communicating, transacting, sending and receiving messages, sharing documents and pictures by using wireless connections. So we can't come out of it. Even though security protocols and their versions are modified to the great extent to make the network secure, hackers are finding different ways to break the code and heisting the data. If we take few precautions we may be some- what secure for a minimal time. Some precautions are:

1. Think before connecting to a free Wi-Fi network.
2. Switch off your Wi-Fi routers when not in use.

Finally I conclude that WPA+AES is the best and more secured version of wireless encryption protocol for the contemporary generation of networks.

Cite this article as :

A. Sruthi , "Cyber Encryption ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 79-82, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194714