An overview on wired vs wireless modes of internet,and security protocols used for wireless network communications.

Prepared by Sameer Singh and Oluwakeye Oluwafikayo

April,2022

Contents

1 Introduction

A network consists of 2 or more computers that are linked in order to share resources, exchange files or allow communication electronically. These systems can be connected either through cables or through a wireless connection. The simplest network typically involves 2 systems connected by a cable and this is called a peer to peer connection. In this connection, there is no hierarchy as both systems both have equal privileges in the network. Nowadays, networks are more complex as they now involve more computers connected to a single network. These are called client-server networks.

2 Network Topology

The topology of a network is the arrangement of the network which consists of a sender and the receiver connected together by nodes. They are 5 different of topology namely:

1. Mesh topology.
2. Star topology.
3. Bus topology
4. Ring topology
5. Tree topology.

2.1 Mesh Topology

In this topology, devices are connected to each other using dedicated channels which are known as links. For N number of systems connected to the network, the number of ports for each system is N-1 and the total number of ports is N*(N-1).

2.1.1 Advantages

It is robust. It provides security and privacy.

2.1.2 Disadvantages

Cost of implementation and maintenance is high.

2.2 Star Topology

In this topology, all devices are connected to a single hub and get their resources from the hub. The hub can either be a passive or active hub.

Advantages It is easy to set up It does not require more than N ports.. **Disadvantages** Cost of installation is high. If the hub fails,the entire topology fails.

2.3 Bus Topology

In this topology all devices are connected to a single cable and get their resources from the cable as data is being transferred from one end to the other.

Advantages Cost to setup is low. **Disadvantages** Failure of the common cable results in failure of the entire cable. Security is low.

2.4 Ring Topology

In this topology devices are connected together to form a ring. Repeaters are added to this topology in order to prevent data loss due to the distance it takes to transfer data.

Advantages Possibility of data collision is minimal Installation cost is low. **Disadvantages** Difficult to troubleshoot errors in this topology. Less secure. Difficult to add or remove devices from it.

2.5 Tree Topology

This is a variation of the star topology as data is transferred from top to bottom. There is a central hub in this topology which then has various secondary hubs which then connect to the various devices. **Advantages** Distance between devices and the central hub is shortened. Allows for isolation and prioritization of devices **Disadvantages** Cost of implementation and maintenance is high. If the central hub fails, the entire hub will fail.

2.6 Components of a network

For a network to function, there are various components that have to be present and they will be discussed based on two parts:

1. Physical Components
2. Software components

2.6.1 Physical Components

These components are parts of the network which can be seen and they are 5 physical components in a network:

1. **Servers**- The servers are high configuration computers which manage the resources of the network. They are used to process client requests and provide appropriate responses. They contain the network operating system which enables the servers to control what clients can access across the network.
2. **Clients** - The clients are basically the computers which request and receive service from the servers to access and use the network's resources. It is

important to note that a server also can become a client anytime it needs to go on to the network and initiate communication.

3. **Peers**- A peer in a network is a node that provides the same functionality as another. This occurs between 2 systems which act as both clients and servers at the same time without the need to involve a centralized server.

4. **Transmission Media**- This refers to the channels through which data is transferred from one device to the other. They can be in the form of cables in wired networks or microwaves and infrared waves in wireless connections.

5. **Connecting Devices**- These are devices which act as middlemen between networks. They include devices such as routers, bridges, hubs, gateways, repeaters and switches. Each of these devices are used to build and design specific types of networks with solid security that serves the individual or business well.

2.6.2 Software Components

1. **Networking Operating system(NOS)**-This system is designed to support workstations, personal computers and older terminals.It allows multiple devices within a network to communicate and share resources. The system is usually embedded in the server which in turn gives the server the ability to allow or restrict devices from communicating on the network. The NOS has 2 types which are the peer to peer and the client server.

2. **Protocol suite**- This is the guideline in which all the clients follow for data communication.There are various network protocols being used in today's networking environment but the 2 popular protocol suites are: OSI model and TCP/IP model.

2.6.3 OSI model

This model splits communication into 7 layers. They various layers are:

(a) **Physical layer**- This layer is the interface between the network and its devices.

(b) **Data link layer** - This layer frames packets and detects packet transmission errors.It is split into 2 protocols: ARP(address resolution protocol) - This protocol helps map IP addresses to physical machine addresses recognized in the local network. SLIP(Serial line Ips) - This protocol is used for point to point serial connections. It enables a combination of hosts and routers to communicate with each other.

(c) **Network layer**- This layer routes packets according to unique network device addresses. Examples of these protocols are: IPSec(internet protocol secure) and VPNs - This protocol provides authentication, integrity and data privacy between any 2 systems. It is used to set up VPNs by encrypting ip packets and authenticating the source where the packets are from. A VPN is an encrypted connection between 2 or more computers. It makes it possible to access and exchange data confidentially over shared network infrastructure. This is useful for companies whose employees work remotely. SSL (Secure sockets Layer) and TLS - The SSL ensures the data transferred between the client and the server is private and also ensures the client can authenticate the identity of the server. The process involved in this protocol is based on a security handshake between the client and the server and both agreeing on the security keys and algorithms to use for encryption. SSL encrypts and decrypts all information in the server response and the HTTPS request including the URL, contents of the submitted form, usernames, passwords and the data being sent. Unfortunately, this protocol is now deprecated and has been succeeded by the new protocol TLS(transport layer security). This protocol is also used in encrypting communication between web applications and servers and evolved from the SSL protocol. It is mainly the same method used in both protocols; the only difference is the change in name of the protocol.

(d) **Transport layer**- This manages end to end delivery in networks. It also renders reliable and sequential packet delivery using flow and error recovery mechanisms. Examples include TCP(transmission control protocol) - It is a delivery connection service which requires a connection between the ap[ploications before data can be transferred. UDP(user datagram protocol) - It is the opposite of TCP as it does not require a connection between the applications before data is transferred. It is less reliable than the TCP protocol.

(e) **Session layer**- It manages user sessions which includes establishing and terminating sessions between users. Examples of protocol include RPC (remote procedure call protocol) -This protocol is used to request service from a program in the computer connected to the network.

(f) **Presentation layer**-It masks the differences in data formats , encodes and decodes , encrypts and decrypts , compresses and decompresses data. The protocol involved in this layer is the LPP(lightweight presentation protocol) which provides support for application services.

(g) **Application Layer** - This provides services such as terminals, files and job transfer operations. Protocols in this layer includes: DHCP (dynamic host configuration protocol), DNS (domain name system

protocol), FTP (file transfer protocol), HTTP (Hypertext transfer protocol).

2.6.4 TCP /IP Model

This model is a concise model of the OSI model. Unlike the OSI model, it has 4 layers. The layers are :

(a) **Process/Application layer**- This layer is a combination of layer 1 (Physical layer) and layer 2 (Data link layer) of the OSI model). It consists of the same protocols in both layers of the OSI model.

(b) **Internet layer** -This layer is equivalent to the network layer of the OSI model and is responsible for transmission of data over the network.

(c) **Host to host layer** -This is equivalent to the transport layer of the OSI model which is responsible for end to end communication and error free delivery of data.

(d) **Network access/link layer**- This is a combination of the top three layers of the OSI model(application, presentation and session layer). It is responsible for node to node communication and controls user-interface specifications.

2.7 Wired And Wireless Networks

As seen from the previous chapter, a network is a set of communication devices that are connected in order to share resources, exchange files and allow electronic communications. The network was designed in 1972 and developed in 1980 under the IEEE standards. The network can be broken down into 2 types which are the local area network and the wide area networks. The local area network is a network which is confined to a small area while a wide area network as the name suggests is confined to a larger area. In these 2 types of network, we will take a look at the ways in which data can be transferred within them. The first mode is the wired mode of transfer which involves cables which establish connection to the internet and other devices on the network. These cables usually consist of copper, fiber optic and twisted pairs and are called ethernet cables. Examples of these cables include Cat5, Cat6 e.t.c. Although the wireless network which will be talked about later is the most prominent mode of data transfer, the wired mode is still used for some intensive tasks such as streaming services and virtual communication.There are majorly 3 types of wired ethernet:

1. **Fast Ethernet** - This type of ethernet connection offers high speeds of about 100 megabits per second when data is being transferred. A Cat5 cable is usually required for this type of connection. It was launched in

1995 and was the fastest connection at that time.The range of this ethernet can be from 400 yards to 25 miles.

2. **Gigabit Ethernet** - This is an upgrade from the fast ethernet. If the speed of the fast ethernet is not offering the needed requirements, the gigabit ethernet is considered as it offers a speed of 1000 megabits per second. This type of wired ethernet is replacing the fast ethernet and slowly phasing it out as now home networks already come equipped with it. It supports video streaming and more advanced tasks.

3. **10-Gigabit Ethernet** - This type offers speed of 10 gigabit per second. For this type of ethernet, a Cat7 twisted pair cable is used or any other fiber optic cable. It is not mainly adopted as of now due to its high cost and is mostly limited to core and large data networks. It is a full duplex mode which enables the transmission of data in both directions simultaneously. It offers data transfer for distances of up to 40 kilometers on single mode fiber and up to 300 meters on multimode fiber.

Wireless network is the opposite of a wired network based on the fact that it is based upon a frequency without using any form of wire. Electromagnetic waves or infrared waves are used for the transfer of data.The first wireless network was developed in 1969 at the university of Hawaii. Examples of wireless networks include cell phone networks, wireless local area networks e.t.c. Types of wireless networks:

1. **Wireless PAN(WPAN):**This wireless network connects devices within a relatively small area.

2. **Wireless LAN(WLAN):**This links two or more devices over a short distance using a wireless distribution method.

3. **Wireless ad hoc network:**This network is made up of radio nodes organized in a mesh topology. Each node forwards messages on behalf of the other nodes.

4. **Wireless MAN:**Also known as wireless metropolitan area network which connects several wireless LANs together.

5. **Wireless WAN:**Wireless wide area networks are networks that cover large areas such as neighboring areas, cities and suburbs.

6. **Cellular network:**It is a radio network distributed over land areas called cells which is served by at least one fixed location transceiver.

7. **Global area network:**This is a network used for supporting mobile across a random number of wireless LANS.

8. **Space network:**These networks are used for communication between spacecraft.

Now that a basis has been set on what a wired and wireless connection is, We can now take a look into the advantages and disadvantages of these forms of transferring data. The table below gives a list of the advantages of both networks and the disadvantages of these connections.

2.7.1 Advantages and Disadvantages of wired and wireless networks

The advantages of both methods are:

Wireless Connection	Wired Connection
There is freedom of movement and ease of access within the area of the network.	Has more control over permissions due to having permission of how many devices can connect to the network.
Easier to share files with other devices connected to the network	Greater control over the security protocols of every device connected to the network.
Cost of setup is lower due to the lack of having to purchase cables and other equipment to implement wired connection	It is faster than wireless networks due to it having a direct connection to the internet.Also due to it having a better bandwidth and faster transfer speeds.
Ease of adding new devices to the network without having to get cables	-
It accommodates more users due to the lack of restrictions based on the number of ports.	-

The disadvantages of both methods are:

Wireless Connection	Wired Connection
The speed is slower than the wired networks.	Installation is complex and lengthy.
Distance from the router is a major factor to the functionality of the network.	Maintenance requires a lot of time and expense.
They are less secure and easier to hack Inconsistent in terms of connectivity and speed.	Hard to keep components such as cables organized and leads to a poor outlook. Limited mobility as one can go as far as the cable permits.

Before we discuss the best method for a business infrastructure, the security of the wireless aspect will be addressed as there are some common misconceptions about the security not being secure. The major reason why it is deemed insecure is majorly in regard to public wireless networks in areas such as cafes and other public areas but for privately owned wireless networks, the network security is mainly decent. Based on the background on the wired and wireless network, we now determine which method is best suited in a business enterprise. Several factors need to be considered before a network connection is applied to a business enterprise and these factors will determine what connection is chosen. The factors taken into consideration are :

1. Permissions.
2. Security.
3. Accessibility.
4. Budget.
5. Number of users.
6. Location of users.
7. Distance of users.

Based on these factors it is easy to realize that the choice of what network to use rests solely on the preference of the business as both methods beat one another out in different aspects. Based on this realization , we narrow down the method in which the decision on what method to use is based. The method used is the measuring of the quality of service which includes traffic sent, traffic received, delay and throughput provided by each network and the security of each network. Based on a research study performed on both the wireless and

wired networks using a simulation tool known as OPNET, it was concluded by KumarBachlas (2014)

After analyzing all above results it has been investigated that the performance of wired Network is better in case of delay because delay is very low in case of wired LAN as compared to wireless LAN. So, in case of low delay and less interference Traffic sent and Traffic received is small in case of wired network but in case of Wireless LAN peaks in graphs represents that Traffic sent is more but traffic received is less in Wireless LAN.(10) This shows that the quality of service provided by the wired network is better than that of the wireless network. Although the test was conducted years back and there has been a lot more advancement in regards to wireless networks, these tests still hold true as wired networks still come out on top in the aspects conducted in the test.

Part 2 of this paper briefly discusses the evolution of wireless network security protocols, followed by a case study on ethical hacking. After a brief description of each protocol, part 2 of this paper discusses WPA3 which uses the Simultaneous Authentication of Equals (Dragonfly Handshake) and shows how WPA3 can be breached by ethical hackers using certain cyber attacks.

3 Wireless network security protocols

A wired internet connection that uses an Ethernet cable is more secure over a wireless network as a physical cable connection is required to access the wired network. Wireless networks, on the other hand, do not need physical access to any socket/cable, enabling anyone to try to maliciously connect to the wireless network. However, over time, many security protocols have been introduced to provide a similar security as a wired internet connection, to a wireless one. These protocols are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), and Wi-Fi Protected Access 3 (WPA3). Although each protocol is more secure than its predecessor, a security breach has recently been found in the latest and presumably the most secure network security protocol WPA3.

3.1 Wired Equivalent Privacy (WEP)

The WEP was introduced in 1999 with a 64-bit encryption implementation, which later increased to 128-bit, with 128-bit encryption WEP being the most common implementation. WEP is a security algorithm that uses the RC4 stream cipher (designed by Ron Rivest in 1987) for confidentiality, and CRC-32 checksum to ensure integrity. The RC4 key in a 64-bit implementation of WEP is formed by concatenating a 24-bit Integrity Check Value (ICV) to a 40-bit key (also known as WEP-40). Since RC4 is a stream cipher, the same key must never be repeated; the purpose of concatenating the ICV is to prevent any repetition of the RC4 traffic key. However, for a 24-bit ICV, it was found that there is a 50 percent probability that the same IV will repeat after 5,000 packets. In August

2001, a cryptanalysis of WEP was published by Scott Fluhrer, Itsik Mantin, and Adi Shamir. In their paper, they illustrated the way the RC4 ciphers and ICV are used in WEP, resulting in a passive attack that can recover the RC4 key after eavesdropping on the network for even a 128-bit ICV. Another prominent attack on the WEP protocol was the Caffe Latte Attack.

3.1.1 Caffe Latte Attack

The Caffe Latte Attack is named so because a WEP key could be obtained from an innocent client at a coffee bar in the time it takes to drink your cafe latte by using this attack. "Briefly, this is done by capturing an ARP packet from the client, manipulating it and then send it back to the client. The client in turn generates packets which can be captured by airodump-ng. Subsequently, aircrack-ng can be used to determine the WEP key."
In 2001, Nikita Borisov Ian Goldberg and David Wagner published a paper titled "Intercepting Mobile Communications: The Insecurity of 802.11"which highlighted various inherent flaws of using the WEP protocol. The paper shows that it is possible to inject arbitrary packets into the network, and these packets will be valid encrypted packets and will be accepted by devices on the network. Recall that WEP uses a CRC-32 checksum to ensure integrity. Now, since CRC-32 is a linear function of the message, the checksum is distributive over the XOR operation in the encryption process. Thus, if we carefully tamper arbitrary byte locations in the packet and patch the checksum accordingly, the resulting packet will be accepted by the access point.
To do so, the attacker would need a WEP encrypted packet to create a bitmask. Then, the same CRC-32 algorithm used in WEP is used on that bitmask to get an ICV patch for that bitmask. Now, if the original encrypted packet is XOR'ed with the bitmask and the ICV patch, the resulting packet would contain the modified encrypted data segment and the encrypted ICV segment, and would also be a valid encrypted packet. Mathematically we can represent this as follows:
We know that the XOR operation is distributive. That is,
$(P \oplus K) \oplus A = (P \oplus A) \oplus K$
Let P represent the plaintext data concatenated with its ICV. Let K represent the RC4 keystream. Let A represent the bitmask created by the attacker concatenated with the ICV patch.
The above equation shows that even though the plaintext is not known to the attacker, by XOR'ing the bitmask (and the ICV patch) to the encrypted packet, the resulting modified packet would behave as if the bitmask (and ICV patch) were XOR'ed with the plaintext (and original ICV) and then encrypted (because encryption simply involves XOR'ing the plaintext+ICV with the RC4 keystream). This is why the output packet containing data modified by the attacker is always a valid WEP encrypted packet. Now since there is no mutual authentication in WEP (only the client needs to authenticate itself), an attacker can easily get the client to send WEP encrypted data packets (note that the server, in this case, the attacker does not need to authenticate itself in

WEP encryption) by using tools such as airodump-ng. Once the attacker has accumulated enough data packets, tools such as aircrack-ng can be employed to crack the WEP key.
The Caffe Latte attack has made cracking the WEP key a matter of a few minutes, thereby posing a serious risk to the security aspect. Due to the security flaws and vulnerabilities present in WEP, it was eventually replaced by the Wi-Fi Protected Access (WPA) protocol.

4 Wi-Fi Protected Access (WPA)

The Wi-Fi Protected Access (WPA) was introduced in 2003 as a temporary replacement over the WEP protocol. Since all of the hardware up to that point used WEP protocol, the WPA was introduced as an interim solution to provide security without replacing legacy hardware until hardware could be upgraded to support more secure protocols and algorithms.
WPA uses the Temporal Key Integrity Protocol (TKIP) which introduced 3 new security features:
(a) In WPA, a key mixing function is implemented by the TKIP that combines the root key with the ICV before passing it to the RC4 cipher in contrast to WEP where the ICV was simply concatenated after the root key.
(b) WPA implements a sequence counter that protects against replay attacks and out-of-order packets are rejected by the access point.
(c) A 64-bit Message Integrity Check (MIC) is also implemented by the TKIP that ensures data integrity. It is also referred to as a Message Authentication Code (MAC) (not to be confused with Media Access Control), hash, or a checksum. The MIC also re-initializes the sequence counter each time a new key is used. Depending on the needs of the user, different versions of WPA are available for use.

4.1 WPA-Personal

WPA-Personal, also referred to as WPA-PSK (pre-shared key) mode, was designed for personal networks where an authentication server is not needed. As the name suggests, in WPA-PSK, there is a pre-shared key which the user must know to attempt to connect to the network. This pre-shared key is a 256-bit key which may be entered either as a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters. Each wireless network device connected to the WPA-PSK network encrypts the network traffic by deriving its unique 128-bit encryption key from the 256-bit pre-shared key. If ASCII characters are used, the 256-bit key is calculated by applying the PBKDF2 key derivation function to the passphrase, using the SSID of the network as the salt and 4096 iterations of HMAC-SHA1.
“A key derivation function (KDF) is a cryptographic algorithm that derives one or more secret keys from a passphrase using a pseudorandom function (which typically uses a cryptographic hash function or block cipher).” PBKDF2 applies

a pseudorandom function, in this case HMAC-SHA1, to the input passphrase along with a salt value (which is simply an additional input to a one-way hash function), in this case the SSID and repeats the process multiple times, in this case 4096 times, to produce a derived key. This key can then be used as a cryptographic key in any further operations and functions.
HMAC-SHA1 (Hash-based Message Authentication Code - Secure Hash Algorithm 1) is a cryptographic hash function that outputs a 160-bit hash value, also known as the message digest. "The HMAC process mixes a secret key with the message data, hashes the result with the hash function, mixes that hash value with the secret key again, and then applies the hash function a second time. The output hash is 160 bits in length."

4.2 WPA-Enterprise

WPA-Enterprise, referred to as WPA (as opposed to WPA-PSK used for personal purposes) was designed for enterprise networks. It requires the use of an authentication server such as RADIUS (Remote Authentication Dial-In User Service). RADIUS is a networking protocol developed by Livingston Enterprises in 1991 that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. RADIUS runs on the application layer of the OSI model and is typically transported over UDP/IP on ports 1812 and 1813. In 2012, it was upgraded to be able to use TCP along with TLS on the transport layer of the OSI model.
WPA-personal and WPA-enterprise are available for all further versions of WPA as well. The use of an authentication server provides additional security against attacks such as dictionary attacks on short passwords. Various kinds of the Extensible Authentication Protocol (EAP) are used for authentication. Security measures such as using the MIC, per-packet key hashing, broadcast key rotation, and a sequence counter discourage many attacks used against WEP, and the key mixing function eliminates the WEP key recovery attacks; however since WPA uses the same underlying principles (such as using an RC4 cipher), it still is not secure enough, and a new more secure protocol was needed.

4.3 Wi-Fi Protected Access 2 (WPA2)

The Wi-Fi Protected Access 2 (WPA2) was introduced in 2004 to replace the WPA protocol. WPA2 introduced the Advanced Encryption Standard (AES). WPA2 includes mandatory support for Cipher block Chaining MAC Protocol (CCMP), which is an AES-based encryption mode.

4.3.1 Advanced Encryption Standard (AES)

AES is a 128-bit symmetric block cipher that uses a 128-bit, 192-bit or a 256-bit key for encryption. The plaintext is divided into blocks, each of size 128-bits (16 bytes). These blocks are then arranged in a 4x4 matrix where each of the

16 elements in the matrix corresponds to one byte of the 128-bit block. This data block is also known as the state of the AES. There are 9/11/13 rounds or iterations of the following operations applied to the state:

Byte substitution
This involves a simple substitution of each byte in the AES state by using the AES S-box

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

(Figure 1).
For example, consider the value in the AES state to be 0x9a. Now, we look up row "9" and column "a" of the S-box. The corresponding value in the S-box is b8. Therefore, the byte 0x9a will be converted into 0xb8.
Shift rows This step permutes the bytes between columns because the AES state is processed column-wise. In this step, a circular byte shift is performed in this manner: – 1st row is unchanged – 2nd row does 1 byte circular shift to left – 3rd row does 2 byte circular shift to left – 4th row does 3 byte circular shift to left
Mix columns Each column is processed separately where each byte for every column is replaced by a value that depends on all 4 bytes present in that column. Each column can be expressed as 4 equations (to derive each byte in that column).
Add round key In the final step, the AES state is XOR'ed with 128 bits of the round key processed by column. Decryption is done in a similar manner, where each step is reversed accordingly (for example, in row shifting step for decryption, the rows are shifted right instead of left). An inverse S-box is used instead of the S-box for decryption. The inverse S-box is given in Figure 2.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
10	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
20	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
30	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
40	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
50	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
60	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
70	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
80	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
90	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a0	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b0	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c0	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d0	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e0	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f0	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Certification for WAP2 began in September, 2004. From March 13, 2006, to June 30, 2020, WPA2 certification was mandatory for all new devices to bear the Wi-Fi trademark.

4.4 Wi-Fi Protected Access 3 (WPA3)

Wi-Fi Protected Access 3 (WPA3) is the latest wireless security protocol. Introduced in January 2018, WPA3 was announced as a replacement to WPA2 by the Wi-Fi Alliance, and WPA3 certification began in June 2018. Although WPA and WPA2 addressed and fixed many vulnerabilities present in WEP, perfect forward secrecy was still not achieved. This means that if an attacker is able to obtain a server's private key, they can use that key to decrypt any data sent to the server. The WPA3 fixed this problem by introducing the Simultaneous Authentication of Equals (SAE) exchange, thereby increasing forward secrecy. However even after fixing the security flaws in previous versions, Mathy Vanhoef and Eyal Ronen discovered in 2020 that WPA3 is still not secure.

4.5 Simultaneous Authentication of Equals (SAE)

Simultaneous Authentication of Equals (SAE), also referred to as "Dragonfly Key Exchange" is a new authentication method used in WPA3. "Using SAE, authentication is performed with a hash of a generated key that is unique to each authentication, rather than having the same Pairwise Master Key every time." This enables the Access Point and station peers to authenticate each other during the handshake process, while using cryptographic tools to prevent an attacker from performing an offline password cracking scheme. For compatibility

purposes, SAE allows WPA2 clients to be connected to a network which uses WPA3. A user can do so by using the transition mode configuration of WPA3. SAE uses a key-based technique known as Elliptic Curve Cryptography (ECC) for encrypting data. ECC is an alternative technique to the RSA algorithm that generates security between key pairs for public key encryption by using mathematical properties of elliptic curves. Lochter, M. and J. Merkle introduce a new set of elliptic curve groups called ECC Brainpool curves over finite prime fields for use in cryptographic applications. (7) These ECC brainpool curves are used in SAE during encryption.

5 Ethical hacking: Case study

Hacking/hackers are usually associated with a malicious aim. However, not every instance of hacking is done with a hostile intent. In a cyber security context, a network security hacker can be defined as an individual who is able to gain unauthorized access to secured data, or has the ability to launch cyber attacks targeting specific individuals or groups. In this section, the term "hacker" will be used synonymously with "network security hacker". Section 2.1 lists some commonly encountered types of hackers including white hat hackers (ethical hackers). Ethical hackers are further discussed in Section 2.2, which focuses on ethical hacking. Section 2.3 examines some cyber attacks used by ethical hackers to test network security.

5.1 Classification of security hackers

Over time, multiple terms have been used to categorize network security hackers. The most frequently discussed and relevant categories of security hackers are white hat hackers (ethical hackers), black hat hackers (threat actors), and gray hat hackers. Hackers that do not fit any of these labels may be classified as red hat hackers, blue hat hackers, hacktivists, and script kiddies among other subgroups.

Black hat hackers (threat actors)

Black hat hackers, also known as threat actors are the malicious hackers who use hacking tools and techniques illegally for selfish gain. Some common cyber attacks carried out by black hat hackers include phishing, infecting a user on the network with malware such as ransomware and Trojan, Denial of Service/Distributed Denial of Service DoS/DDoS attacks, database injection, etc.

White hat hackers (ethical hackers)

White hat hackers, also known as ethical hackers are the network security professionals who use hacking for testing their own security systems, or may sometimes be employed by an organization to test their network security.

Grey hat hackers

Grey hat hackers can be thought of as a blend of white hat hackers and black hat hackers. Grey hat hackers are not employed by any organization, but use their skills to discover vulnerabilities of a system. They may then choose to

report the flaws to the administrator, or publish them online. Although not all hackers belonging to this category have a malicious intent, unauthorized access to systems is illegal, and grey hat hackers should be encouraged to get certified as an ethical hacker and use their skills for development as a white hat hacker.

Red hat hackers

Red hat hackers use their skills to stop black hat hackers from carrying out cyber attacks. Although they may not have harmful intentions, red hat hackers do not consider the consequences and use any means necessary to target black hat hackers. They may be thought of as vigilante hackers who believe that the ends justify the means.

Blue hat hackers

Blue hat hackers are network security professionals who are invited by various companies in the tech industry before launching a new product to test its security and perform a vulnerability assessment. They are different from white hat hackers as they are not actually an employee of the said company, but simply invited to perform a security check.

Hactivists

Hacktivists are skilled hackers who use their skills and knowledge to carry out cyber attacks to support a point of view, targeting large entities such as the government, entire industries, or may focus on a specific organization, firm, establishment, etc. Usually, they strive to cause a social change, or promote a political agenda.

Script kiddies

The term "Script Kiddie" is assigned to an individual who with little or no technical knowledge uses publicly available programs, scripts, etc. to gain unauthorized access for selfish gain. The findings of researchers from Kaspersky Antivirus published in an article by John Oates, titled "Back-2-school hacking: Kaspersky blames pesky script kiddies for rash of DDoS cyber hooliganism" suggest that a large number of cyber incidents have been caused by students acting as script kiddies. "60 per cent of stopped attacks were against either schools, universities or electronic journals – led Kaspersky to believe that students are to blame for the uptick.".

5.2 Ethical Hacking

Ethical hacking is a branch of information security, in which ethical hackers use tools and techniques to find flaws and threats in a system or network. In their paper titled "Study Of Ethical Hacking" Sahare et. al. define ethical hacking as an identical activity which aims to find and rectify the weakness and vulnerabilities in a system.Their paper elaborates ethical hacking in detail explaining the types of ethical hacking and the impact of hacking on businesses and governments.

Many organizations have private or confidential data that can be maliciously accessed by hackers. These organizations may employ ethical hackers to conduct tests such penetration testing or use cyber attacks against their network to diagnose security flaws. Bacudio et al, define penetration testing as a series

of activities undertaken to identify and exploit security vulnerabilities.Their paper provides an overview of penetration testing by discussing its benefits, the strategies and the methodology of conducting penetration testing. Some cyber attacks used by ethical hackers are discussed in the next section.

5.3 Common cyber attacks used by ethical hackers

Downgrade attack
As the name suggests, a downgrade attack "downgrades" the attacked protocol, making it roll back to a previous less secure version so that another cyber attack can be launched which may not have otherwise been possible on the upgraded protocol. Often, the only solution to prevent downgrade attacks is to remove backward compatibility of the system.
Brute Force Attack
A brute-force attack is the most basic type of cyber-attack. It involves the attacker simply inputting all the possible permutations of a secret key/passcode/password until the correct key is obtained. Theoretically, brute-force can be used to decrypt any data. However, since it involves every permutation of the key possible, as the key size increases, the number of possible permutations increases.

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/μs	Time required at 10^6 decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	6.4×10^6 years

The above table shows that a simple brute-force attack is usually not practical. Therefore, brute-force is often used in combination with another type of cyber-attack.
Dictionary attack A dictionary attack is a type of brute-force attack in which instead of using all possible permutations of a password/key, only select permutations are used. A premade library which lists some permutations of the secret key is used in a dictionary attack. Keys listed in that library are used as input key in a brute-force manner.
Denial of Service (DoS) attack A Denial of Service (DoS) attack is a cyber attack in which the attacker floods a system/network with data, causing the network to shut down, or by sending invalid data that triggers a system crash. When the DoS attack is carried out by multiple systems, each targeting the same network, it is known as a Distributed Denial of Service (DDoS) attack. A successful DoS/DDoS attack renders the targeted network/service inaccessible

for any user.
Side-channel attack A side-channel attack uses the knowledge about the implementation of the targeted system rather than exploiting known vulnerabilities like software bugs. Some side-channel attacks include cache attacks, timing attacks, electromagnetic attacks, etc.
Timing attack A timing attack is a side-channel attack in which the attacker analyzes the time taken by the targeted system to execute certain cryptographic algorithms, with the purpose of breaching that system. Based on the time difference it takes for the system to run these algorithms, the attacker can reverse-engineer the inputs used and eventually gain unauthorized access.

6 Shortcomings of WPA3

On May 18, 2020 Mathy Vanhoef and Eyal Ronen presented their paper titled " Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd" at the IEEE Symposium on Security and Privacy. In their paper, they showed that although WPA3 uses the Dragonfly handshake, it is still possible for an attacker within range of a victim to recover the password of the network.They used downgrade attacks to roll back a WPA3 network to a WPA2 network and carry out dictionary attacks on the victim authenticated WPA2 4-way handshake. The high cost of the Dragonfly handshake was then exploited by performing a DoS attack to abuse the high overhead cost. Side channel attacks including timing attacks and cache-based side channel attacks were carried out against the brainpool curves used in WPA3, to reveal information about the password. This information is used to carry out dictionary attacks/brute force attacks to compute the password.
In their paper, Vanhoef and Ronen suggest some changes to the Dragonfly's password encoding algorithm. "In particular, the peer's MAC addresses (i.e. identities) can be excluded from the password encoding algorithm, and instead included later on in the handshake. For EAP-pwd the server's random token must also be excluded.
This allows the password element to be computed offline, meaning an attacker can no longer actively trigger executions of the password encoding method. It also means that for a given password the execution time of the password encoding method is always the same, limiting the amount of info being leaked, which cannot help an attacker to guess the password by much." Their changes can be implemented to create a more secure wireless network security protocol.

7 References

(1) Aircra(2010). Cafe Latte attack. Aircrack-ng. Retrieved April 7, 2022, from hck-ng. ttps://www.aircrack-ng.org/doku.php?id=cafe-latte.

(2) Bachlas, K. A. (2014). Comparative Analysis of Wired and Wireless Lan Network QOS Using OPNET as Simulation Tool. Academia.

(3) Borisov, N., Goldberg, I., amp; Wagner, D. (2001, August 1). Intercepting Mobile Communications: The Insecurity of 802.11. Retrieved April 8, 2022, from http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

(4) Bacudio, A. G., Yuan, X., Bill Chu, B. T., amp; Jones, M. (2011, November). An Overview of Penetration Testing. Retrieved April 8, 2022, from https://www.researchgate.net/publication/274174058AnOverviewofPenetrationTesting

(5) Dotnet-Bot. (2018). HMACSHA1 Class . (System.Security.Cryptography) — Microsoft Docs. Retrieved April 8, 2022, from https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.hmacsha1?view=net-6.0

(6) Fluhrer, S. R., Mantin, I., amp; Shamir, A. (2001). Weaknesses in the Key Scheduling Algorithm of RC4. Retrieved April 4, 2022, from https://www.cs.cornell.edu/people/egs/615/rc4ksaproc.pdf.

(7) Khan, R. A., Tariq, M. A. (2019, April 9). A survey on wired and wireless Network. Researchgate. https://www.researchgate.net/publication/332319614ASurveyonWiredandWirelessNetwork.

(8) ManageEngine, communications@manageengine.com. (n.d.). Network Monitoring Software by. ManageEngine OpManager. https://www.manageengine.com/network-monitoring/network-protocols.html.

(9) Mathy Vanhoef and Eyal Ronen. 2020. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In IEEE Symposium on Security Privacy (SP). IEEE.

(10) Merkle, J., amp; Lochter, M. (2010, March). RFC 5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. Retrieved April 8, 2022, from https://datatracker.ietf.org/doc/html/rfc5639

(11) Oates, J. (2019, November 11). Back-2-school hacking: Kaspersky blames pesky script kiddies for rash of DDoS cyber hooliganism. The Register® . Retrieved April 8, 2022, from https://www.theregister.com/2019/11/11/kidsblamedforddosspikeinseptember/

(12) Sahare, B, Naik, A., amp; Khandey, S. (2014). Study Of Ethical Hacking. Retrieved April 8, 2022, from http://www.ijcstjournal.org/volume-2/issue-6/IJCST-V2I6P2.pdf

(13) T. (2021, October 29). Wired vs wireless internet: The pros and cons. Techaeris. https://techaeris.com/2021/10/29/wired-vs-wireless-internet-the-pros-and-cons/.

(14) Wikimedia Foundation. (2022, March 28). Key derivation function. Wikipedia. Retrieved April 8, 2022, from https://en.wikipedia.org/wiki/Keyderivationfunction

(15) What is a Wireless Network? - Wired vs Wireless. (2021, July 1). Cisco. https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/wireless-network.html.

(16) What is WPA3 and what you should test in WPA3 enabled devices. QA CAFE. (2019, August 24). Retrieved April 8, 2022, from https://www.qacafe.com/resources/what-is-wpa3-how-to-test-wifi/

(17) What is a network? Definition, explanation, and examples. (2021, December 8). IONOS Digitalguide, from https://www.ionos.ca/digitalguide/server/know-how/what-is-a-network/.