|  |
| --- |
| The Billericay School |
| How can computer networks be improved and how can they be secured more efficiently? |
| **Trina Roy** |
| **10/18/2016** |

|  |
| --- |
| I am going to discuss what are computer networks and how can they be secured more efficiently. |

Contents

[Introduction 3](#_Toc474137470)

[LANs 3](#_Toc474137471)

[WANs 3](#_Toc474137472)

[Internet 3](#_Toc474137473)

[MANs 3](#_Toc474137474)

[PANs 4](#_Toc474137475)

[Peer-to-peer 4](#_Toc474137476)

[Client – server 4](#_Toc474137477)

[Network topology 5](#_Toc474137478)

[Bus network topology 5](#_Toc474137479)

[Ring network topology 5](#_Toc474137480)

[Star network topology 6](#_Toc474137481)

[Mesh network topology 6](#_Toc474137482)

[Hybrid network topology 7](#_Toc474137483)

[OSI Model 7](#_Toc474137484)

[Physical layer 8](#_Toc474137485)

[Data link layer 8](#_Toc474137486)

[Network layer 8](#_Toc474137487)

[Transport layer 8](#_Toc474137488)

[Session layer 8](#_Toc474137489)

[Presentation layer 8](#_Toc474137490)

[Application layer 9](#_Toc474137491)

[TCP/IP model 9](#_Toc474137492)

[Host to Network layer 9](#_Toc474137493)

[Internet layer 9](#_Toc474137494)

[Transport layer 9](#_Toc474137495)

[Application layer 10](#_Toc474137496)

[Internet security protocols 10](#_Toc474137497)

[SSL 10](#_Toc474137498)

[SHTTP 10](#_Toc474137499)

[3D Secure protocol 10](#_Toc474137500)

[WAP Security 10](#_Toc474137501)

[Security in GSM 11](#_Toc474137502)

[Elements 11](#_Toc474137503)

[Authentication 11](#_Toc474137504)

[Voice and data security 11](#_Toc474137505)

[Security in 3G 11](#_Toc474137506)

[Security in 4G 11](#_Toc474137507)

[Transport Layer and its security 12](#_Toc474137508)

[Information, computer and network security 12](#_Toc474137509)

[Passive attacks 12](#_Toc474137510)

[Wire tapping 12](#_Toc474137511)

[Port Scanner 12](#_Toc474137512)

[Idle scan 12](#_Toc474137513)

[Active attacks 13](#_Toc474137514)

[Phishing 13](#_Toc474137515)

[Man in the middle 13](#_Toc474137516)

[Cross – site scripting 13](#_Toc474137517)

[Cryptography 13](#_Toc474137518)

[Plain and cipher text 13](#_Toc474137519)

[Substitution techniques 13](#_Toc474137520)

[Transposition techniques 13](#_Toc474137521)

[Encryption and decryption 14](#_Toc474137522)

[Steganography 14](#_Toc474137523)

# Introduction

I am conducting research on how we can improve current computer networks, and more importantly in network security.

First, the definition of a computer network. **A computer network is a group of computer or terminals such as workstations, linked together by network cabling or by wireless links.** (Administrator, 2013)1

We utilise networks for sharing data, software and hardware. This helps to communicate easily. There is an abundance of networks, depending on which organisation you are involved in. They are L.A.N, W.A.N, M.A.N and P.A.N. There is also a variety of network topologies. There will be the constant use of the word SERVER and CLIENT**. A server is an instance of a computer program that accepts and responds to requests made by another program, known as a client.** (ComputerHope, 2016)4

## LANs

A LAN (Local Area Network) is a network and it typically covers a small area. The computers are in the same building or in different buildings on one site permanently connected to each other with special cables like school buildings or a small organisation. The communication can be in the form of fibre optic, copper cabling (for the Ethernet) and/or **wireless devices**. There are two types of LANs and WANs: **Peer-to-peer** and **client-server** networks. (Administrator, 2013)1

## WANs

A WAN (Wide Area Network) is a network, which covers a much bigger area geographically and they are not permanently connected to each other by using telephone lines, radio transmitters or satellite links. These are connected by gateways. An example could be the Internet, which is a network of networks – the entire world is connected through it. (Administrator, 2013)1

### Internet

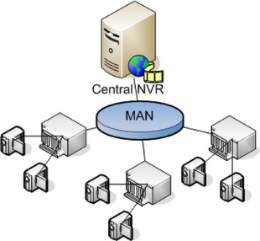
The Internet, as we know it, developed about 59 years ago, in 1957, when the US government created the Advanced Research Projects Agency (ARPA), a part of the Department of Defence fuelled with the responsibility of U.S. leadership in science and technology with military uses. In 1969, ARPA confirmed ARPANET, the predecessor of the Internet. (Duhon & Dartez, 2003)13

ARPANET was a network that was developed for the sole reason of exchanging information from the major computer at the University of California at Los Angeles, the University of California at Santa Barbara, Stanford Research Institute and the University of Utah for computer professionals, engineers and scientists. In a couple of years more and more educational and research, institutions joined the network. (Duhon & Dartez, 2003)13

To reply to the fear of the nuclear attack, ARPANET was created in such a way that it was allowed the continuation even if one or more workstations were destroyed. (Duhon & Dartez, 2003)13

## MANs

A MAN (Metropolitan Area Network) is a big network, which covers a city or a large campus. It can spread over between 5 and 50 km diameter. It can be set up for a specific business, however, it is mainly utilised by many users or organisations. It repeatedly performs as a high-speed network for regional files. In Figure 1, there is a structure of a MAN. (Sinha, S.K & Barman, S.N, 2016) (Kaur, 2010)10



*Figure 1:* Metropolitan Area Network (MAN) (Source: myshubsang.wordpress.com, 2016)

## PANs

PAN (Personal Area Network) is the smallest, in terms of area coverage. It is utilised for personal digital assistant and telephones, or any device, which is in close proximity (individual’s body). In Figure 2, we can see the structure of a PAN, which is formed devices in the home connected together. In Figure 2, there is a possibility of devices, which could be connected in a PAN. (Profandroid.com, 2017) (Kaur, 2010)10

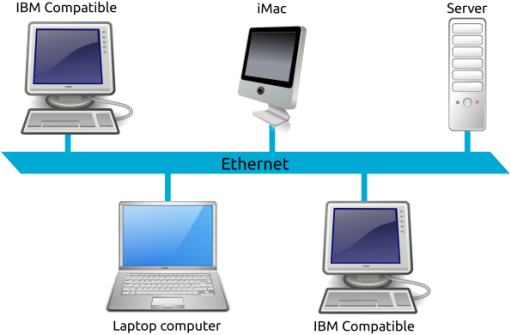
**

*Figure 2:* Personal Area Network (PAN) (Source: Profandroid.com, 2017)

Any network can be set up in a peer-to-peer or client-server network, which are:

## Peer-to-peer

The peer-to-peer network is centralised. All stations in the network have equal status. Each user is responsible for their data, stored on a local disk drive, and not shared. Printers can be attached to a single computer and carry their specific jobs. As you can see in Figure 3, the structure of the peer to peer is quite simple. Figure 3 shows how the network is structured. (Wikipedia, 2015) (Administrator, 2013)1

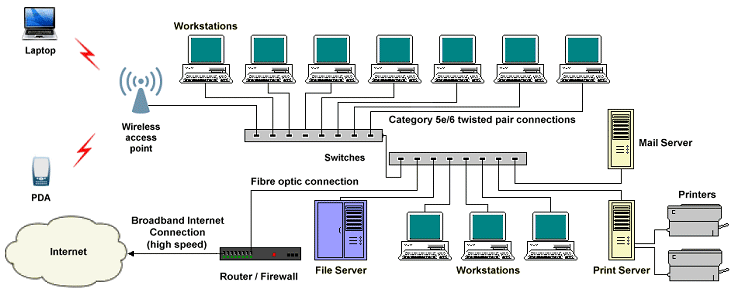


*Figure 3*: Peer – to – peer network (Source: Wikipedia, 2015)

## Client-server

The client-server network is a slightly bigger network e.g. more than five stations. In this case, a server is centralised. Sometimes, the computer can act as a server.

There is also a need for specialised network operation software on the server e.g., Microsoft Small Business Server and it is indispensable that there is a NIC (Network Interface Card). They need specialised setup and support. In Figure 4, it can be seen that client-server networks are developed. (TechnologyUK, 2016) (Administrator, 2013)1



*Figure 4*: Client-server network (Source: TechnologyUK, 2016)

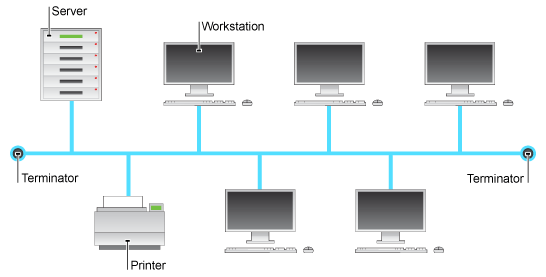
# Network topology

A network topology is how the nodes (computers, printers, routers or other devices) are connected to a network via links e.g. copper wire cable or optical fibre cable, or in simple terms the way the network is set up. (The Linux Information Project, 2005)9

Optical fibre cables are used more often since they have a higher strength than copper. There are four types of topologies: bus, ring, star, mesh (partial or full) or hybrid.

## Bus network topology

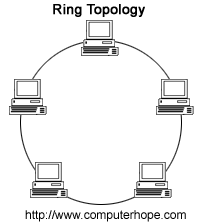
In a bus topology, there is a cable, which is connected to each of the workstations, so if there is a damage to one of the workstation, the rest are unaffected. This is the simplest and less costly to set up. Because of the one connection to all the workstations, this makes the network very slow. In Figure 5 there is a bus topology which shows the simplicity of the topology (BBC Bitesize, 2017) (Administrator, 2013)1



*Figure 5*: Bus topology (Source: BBC Bitesize, 2017)

## Ring network topology

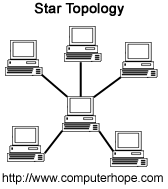
In the ring network topology, every workstation is connected to the next workstation, creating a loop, so if there is a damage in the topology, the whole network will collapse. In Figure 6, it can be seen how a star topology looks like. (ComputerHope, 2017) (Administrator, 2013)1



*Figure 6*: Ring topology (Source: ComputerHope, 2017)

## Star network topology

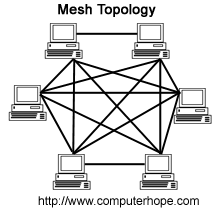
In the star network topology, there is a file server, which is connected to each of the workstations, so if there is a damage to one of the workstation, the rest are unaffected. Nevertheless, if the server is damaged, all the workstations are affected by it. The cost of cabling is quite high. In Figure 7, there is a diagram of a star topology and the costings of it. (ComputerHope, 2017) (Administrator, 2013)1



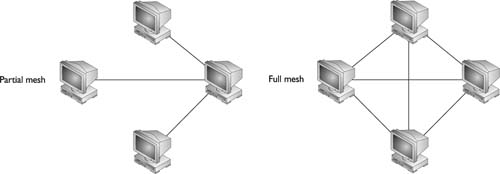
*Figure 7*: Star topology (Source: ComputerHope.com, 2017)

## Mesh network topology

There are two types: Full or Partial. When there is a full mesh topology, all the devices are connected to each other, whereas when there is a partial mesh, some of the devices are connected to others and other devices are connected to other nodes which they share data. Figure-eight shows how a full mesh topology looks like and Figure 9 shows what a partial mesh looks like. (ComputerHope.com, 2017) (Internet of things agenda, 2016)7



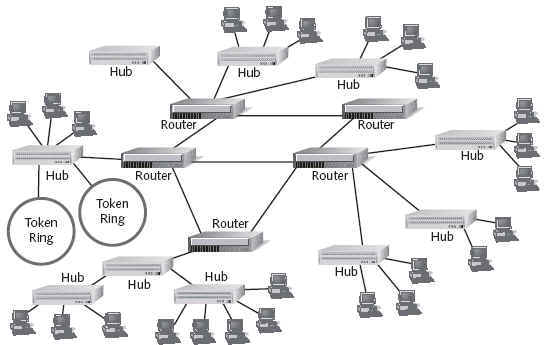
*Figure 8*: Full mesh topology (Source: ComputerHope.com, 2017)



*Figure 9*: Partial mesh topology (Source: ComputerHope.com, 2017)

## Hybrid network topology

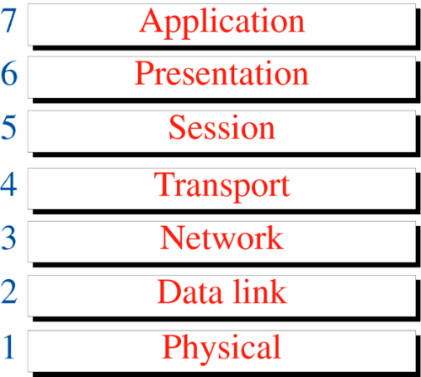
In a hybrid topology, the topology is “mixed up”. What it refers to is that there is a combination of different topologies together, making the file sharing between the businesses much more effective. Alternatively, in another case, it can be the usage of the network design. In Figure 10, it can be seen how does look a hybrid network topology (Reference.com, n.d.)12



*Figure 10*: Hybrid network topology (Source: AngelFire.com, 2017)

# OSI Model

It was formed by a coalition of counties, which were under the International Standards Organisation (ISO). OSI stands for Open System Interconnection. The OSI model is used for the transfer of data between two devices. The OSI Model is structured as shown in Figure 11. There are seven layers in the model. (Forouzan, 2010)3.



*Figure 11*: OSI Model layers (Source: Behrouz Forouzan, 2010)

The reason why the OSI Model is constructed in this way is that the principles dictated that:

*“A layer should be created where a different level of abstraction is needed.”*

*“Each layer should perform a well-defined function.”* In addition, as shown in Figure 11, every layer is assigned a different set of instructions and they perform in a sequence, from seven to one.

*“The function of each layer should be chosen according to the internationally standardised protocols.”*

*“The number of layers should be large enough that distinct functions should not be put in the same layer and small enough that the architecture does not become very complex.”*

This model has been used as a security model. It sets the standards for security procedures and techniques. Some key aspects have to be taken into consideration:

* Authentication
* Access control
* Non – repudiation
* Data integrity
* Confidentiality
* Assurance or availability
* Notarization or signature

## Physical layer

This is the lowest layer in the OSI model. Its function is to connect the physical connection of the two devices. The connection can be made by the use of twisted pair cable. It transfers the data over a communication channel. (Forouzan, 2010)3

## Datalink layer

The data link layer is responsible for the node-to-node delivery of data. It received the data from the network layer and creates frames, add the physical address to the frames and passes the to the physical layer. (Forouzan, 2010)3

It forms by the combination of:

**Logical Link Layer (LLC):** It gives the methods and provides addressing information for communication between network devices.

**Medium Access Control (MAC):** It forms and maintains links between communicating devices.

## Network layer

The network layer is the layer where the packets are transferred from the sender to the recipient across different networks. It also checks all the packets one at a time. An example of this would be when two systems are and joined by routers, and then the network layer is used. (Forouzan, 2010)3

## Transport layer

This layer has the job of making sure that the message is sent across, from source to destination. It also monitors the positioning of the packets as a group, unlike with the network layer, which would have checked all the packets one by one. (Forouzan, 2010)3

## Session layer

The session layer has the responsibility of making sure that the session runs smoothly between the two devices. It also controls the flow of data, so there is a functioning communication system. (Forouzan, 2010)3

## Presentation layer

The presentation layer has the function of checking the syntax and the sense of information between the devices. It was fabricated for data encryption, decryption and compression. (Forouzan, 2010)3

## Application layer

The application layer gives the user interface, so there are a variety of different applications and provides services i.e. access to the network. (Forouzan, 2010)3

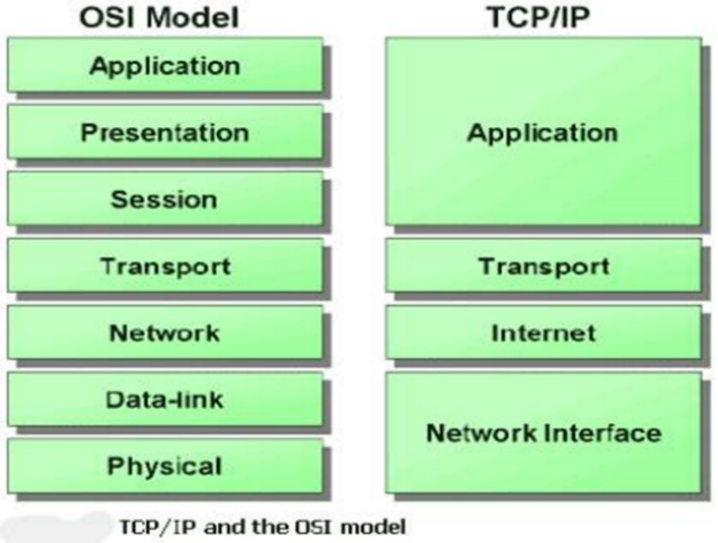
# TCP/IP model

The TCP/IP model is a more recent model that was made. The Internet is based on this model. TCP stands for Transmission Control Protocol and IP stands for Internet Protocol. The design was made by ARPA. (Forouzan, 1998)2

The targets that ARPA wanted to achieve were:

* *“The network should connect multiple networks together.”*
* *“The connection should with till the source and the destination machines are functioning.”*
* *“The architecture should be flexible that it should be able to transfer data among different hardware or software platforms.”*

As you can see in Figure 6 below, the Application layer encapsulates what it would have three layers in the OSI model. This makes the TCP/IP model much more efficient. The network layer in the OSI model is the Internet layer. (Forouzan, 1998)2. In Figure 12, there is an image, which compares the two models. The TCP/IP model is more powerful and more secure than the OSI model.



*Figure 12:* Comparison between the TCP/IP and the OSI model (Source: EazyNotes.com)

## Host to the Network layer

This layer is also known as Network Interface Layer. It is hidden below the internet layer. The target that it has to achieve is to connect the host to the network and sent to the upper layers that they can send the packets. This changes network to network. (Forouzan, 1998)2

## Internet layer

This is similar to the Network layer of the OSI model. It allows the hosts to give the packets to the network and the packets should travel independently using any route. The order in which the packets were sent is not necessarily the same when they are going to be sent, so that is the responsibility of higher layers to make sure that the layers are in the precise order. (Forouzan, 1998)2

## Transport layer

The transport layer in the OSI model and the TCP/IP model have similarities. The transport layer gives the source and the destination workstations to communicate with each other. It separates the byte stream into messages and it controls the flow control so that there is a fast sender should not overflow a slow receiver. (Forouzan, 1998)2

## Application layer

The application layer is essential in the data transfer between applications. It also allows services like e-mail, file transfer, access to the World Wide Web to the user. (Forouzan, 1998)2

# Internet security protocols

## SSL

The Secure Socket Layer (SSL) was created to make secure and reliable access while using TCP. The SSL is two groups of layers of protocols. The SSL Record protocol gives basic security services to higher-level protocols. I am explaining the protocols, which are related to security. (Zele, 2014)15

The SSL Record Protocol gives confidentiality and message integrity for the SSL connection. The message is fragmented into 214 bytes, 16384 bytes, or less.

Compression must be lossless and may extend the content length by up to 1024 bytes.

To authenticate, a code is created over the compressed data. Because of this, a secret key is used.

The Handshake protocol to verify the server and the client and to negotiate an encryption and MAC algorithm and keys to protect the data in an SLL record. (Zele, 2014)15

## SHTTP

The secure hypertext transfer protocol is the groups of techniques defined for protecting Internet traffic. This includes data input forms and internet-based transactions. (Zele, 2014)15

SHTTP and SSL provide similar facilities. Nevertheless, SSL has been utilised more because SHTTP works closely with HTTP, whereas SSL is not. (Zele, 2014)15

It supports both authentication and encryption of HTTP traffic between client and server. (Zele, 2014)15

## 3D Secure protocol

The 3D Secure protocol was developed by Visa after they realised that there was no security when a user wants to provide someone else’s credit card number. Any cardholder has to enrol in the issuer’s bank’s Enrolment server.

Step 1

The user shops on the merchant’s site, and wants to pay the amount. The user enters the credit card details and clicks the OK button. (Zele, 2014)15

Step 2

Once the user clicks OK, the user will be redirected to the issuer bank’s site. The site will create a pop-up screen, prompting the user to enter the password.

## WAP Security

WAP stands for Wireless Application Protocol and it is a stack, including the Wireless Transport Layer Security (WTLS). It deals with the connection between mobile devices and the Internet. The security layer of WAP is an optional layer, as it only functions when the TLS protocol is activated and that only functions when the SSL is functioning. When activated, WTLS functions on top of the transport layer of WAP. WTLS has a similar job as SSL in the wireless world. It protects: (Zele, 2014)15

* Privacy
* Server authentication
* Client authentication
* Data integrity

However, there are issues when there is a conversion between WTLS-SSL, SSL-WTLS is made as to the conversion done on the plaintext, and it is not encrypted.

## Security in GSM

GSM stands for General Packet Radio Service, which is similar AMPS and D-AMPS, the technologies used before. (Zele, 2014)15

### Elements

The SIM has:

* IMSI (International Mobile Subscriber Identity)
* Ki (subscriber authentication key)
* A8 (ciphering key generation algorithm)
* A3 (authentication algorithm)
* PIN (personal identification number)

GSM handset contains:

* A5 (ciphering algorithm)
* AUC (Authentication centre) – part of the GSM network. It has:
  + A3, A5, A8
  + Database of authentication and identification about subscribers

### Authentication

1. Challenge-response authenticates subscriber from the network
2. The network sends 128-bit random number to the subscriber
3. 32-bit signed response using A3 and Ki by the mobile to send to the network.
4. The network finds the value of Ki from the database and performs the same operation with the A3 algorithm
5. If the result matches with one received from mobile, then user authentication is successful.

### Voice and data security

A5 algorithm encrypts voice and data traffic between mobile and network.

The handset sends ciphering mode request to the network.

In response, the network starts encryption and decryption using A5 and Kc (64-bit ciphering key)

## Security in 3G

UMTS (Universal Mobile Telephone System) is the 3G wireless network and it is used for video on demand, video/audio streaming, high-speed multimedia, videoconferencing, and multi-player gaming and improves mobile Internet access. (Zele, 2014)15

The authentication has three parts: user’s mobile, home location and current location (current location can be different from the home location as the user moves around). The user authentication process consists of four steps:

1. The user’s mobile handset sends its International Mobile Subscriber ID (IMSI) to the Home location. The IMSI is unique for a handset and is optionally encrypted before sent to the home location.
2. The home Location performs the following steps now:
   1. It generates a random number (RAND).
   2. Next, it retrieves the secret key it shares with this user’s handset from its database.
   3. It uses the random number and the key to generate the following items:
      1. Response (RES)
      2. Confidentiality Key (CK)
      3. Integrity Key (IK)
      4. Authentication Key (AK)
   4. The Home Location and the user’s handset share a secret, called Sequence Number (SEQ). The Home Location calculates a MAC on the combination of the random number (RAND) and the sequence number (SEQ), i.e. it does MAC (RAND, SEQ).
   5. It now does an XOR operation on the sequence number (SEQ) and Authentication Key (AK), i.e. it does (SEQ XOR AK)
   6. Finally, it sends the following items to the Current Location of the user: RAND, RES, CK, IK, MAC, (SEQ XOR AK)
3. The Current Location receives these values from the Home Location, and sends the following to the user’s handset:
   1. Random number (RAND)
   2. XOR of sequence number (SEQ) and Authentication Key (AK), i.e. (SEQ XOR AK)
   3. MAC
4. The user’s handset receives these values, and performs the following tasks:
   1. It calculates the response (RES), using the random number (RAND) received from the current Location, and the secret key shared with its Home Location.
   2. It also generates various keys such as CK, IK and AK in the same fashion, as was done by the Home Location in step 1.
   3. It now performs an XOR operation using AK over the value (SEQ XOR AK). That is, it performs (SEQ XOR AK) XOR AK. Clearly, this would yield back the sequence number (SEQ).
   4. Using the random number (RAND) and the sequence number (SEQ), it performs a MAC operation, as MAC (RAND, SEQ).
   5. It compares the MAC calculated in step four with the MAC received from the current location (see step 3).
   6. If all these substeps happen successfully, the user’s handset sends the response (RES) to the Current Location. If this response matches with the response (RES) possessed by the current location (recall that it had received this from the home location in step 1), the current location considers this user as authentic and makes the appropriate entries in its database.

## Security in 4G

In Figure 13, there are a variety of issues that the 4G network has, and what can be done to reduce these risks.



*Figure 13*: Security threats and design decisions in a 4G network. (Source: Sumant Ku Mohapatra, Biswa Ranjan Swain and Pravanjan Das)

# Transport Layer and its security

This protocol allows communication around the network, preventing eavesdropping (secret listening of a conversation without consent) and tampering (a device that gives unauthorised access to the protected object). (Zele, 2014)15

It makes sure that privacy between applications and users on the Internet is intact from eavesdropping and tampering.

Two ways it does it:

* Different port number
* Regular port number and request from the client to switch the connection to TLS using a protocol

# Information, computer and network security

## Passive attacks

**Passive attacks** are those wherein the attacker indulges in the monitoring of data transmission. (Zele & Vidya, 2014)14

### Wiretapping

Wiretapping is the surreptitious electronic monitoring of telephone, telegraph, cellular, fax or Internet-based communications. (Whatis.techtarget.com, 2017)16

### Port Scanner

**Port scanner** is a software program designed to go through a large listing of interesting ports or all available network ports and probe for open and accepting packets. (ComputerHope.com, 2017)6

### Idle scan

The **idle scan** is a TCP port scan method that consists of sending spoofed packets to a computer to find out what services are available. (Wikipedia.org, 2017)17

## Active attacks

**Active attacks** are based on the modification of the original message, in some way, or in the creation of a false message. (Zele & Vidya, 2014)14

### Phishing

This is the act of having unauthorised data by commonly using an email system, and entering their sensitive data into a website or form. This will cause identity theft. (Zele, 2014)15

### Man in the middle

A man-in-the-middle attack is an attack where a user gets between the sender and receiver of information and sniffs any information being sent. (ComputerHope.com, 2017)5

### Cross-site scripting

This is the insertion of scripted code into another site’s web page. (Zele, 2014)15

## Cryptography

**Cryptography** is the art of achieving security by encoding messages to make them non-readable. (Zele & Vidya, 2014)14

### Plain and cypher text

**Plain text** is any text, which can be read and understood by the sender, the recipient and anyone else whoever gets the access to the message. (Zele & Vidya, 2014)14

**Cypher text** is the text, which has been codified using any technique. (Zele & Vidya, 2014)14

### Substitution techniques

#### Caesar cypher

The Caesar cypher is the oldest encryption scheme that was ever made. It was coined after Julius Caesar offering the idea of replacing an alphabet with the one three places down. It was the 1st example of substitution cypher. (Zele & Vidya, 2014)14

This is a weak technique to protect data. (Zele & Vidya, 2014)14

#### Monoalphabetic cypher

This is a better cypher as it does not have the *k* positions to try out with the Caesar cypher, as it uses random substitution. Therefore, there are no set rules! (Zele & Vidya, 2014)14

Example: *In a plaintext message, each A can be replaced by any other letter (B through Z), B with A or C through Z. Mathematically, or we can have combinations, which is extremely harder than before.* (Zele & Vidya, 2014)

#### Polyalphabetic cypher

The polyalphabetic cypher uses numerous one-character keys, which encrypt one plaintext character. Once the keys are all used, they are recycled. It uses monoalphabetic rules and uses a key that decides which rule for which transformation. (Zele & Vidya, 2014)14

#### Hill cypher

This cypher works on a different letter at the same time. It was created from the matrix theory of mathematics, focuses on the inverse of a matrix when decrypting. (Zele & Vidya, 2014)14

### Transposition techniques

#### Rail – fence technique

This requires the plaintext to be written as a sequence of diagonals and reading row by row, creating the cypher text. (Zele & Vidya, 2014)14

Example: ORIGINAL TEXT: KILL HIM

K L H M

I L I

Cypher TEXT: KLHMILI

### Encryption and decryption

#### Symmetric and Asymmetric key cryptosystem

**Symmetric key cryptosystem**

The symmetric key cryptosystem is the first type of encryption before the public-key encryption in 1976. (Sivaramkrishnan, 2004)8 It is also known as SECRET KEY, SINGLE KEY, and PRIVATE KEY. (Huth, 2010)11

There are five things in the symmetric key are:

1. **Plaintext:** Text, which is a readable message, or data that is inserted into the algorithm as input.
2. **Encryption algorithm:** It formulates different and permutations on the plaintext.
3. **Secret Key:** The secret key is also added to the encryption algorithm. Depending on the type of changes have been made onto the plaintext and key used, the output will change every time.
4. **Cypher text:** This is the protected message produced as an output.
5. **Decryption Algorithm:** This is the algorithm which is used to decrypt (put it back into) plaintext.

There are some needs when utilising the key:

* The sender and the receiver already share a secret key in a secure way and that they are maintaining their security.
* There is the idea that it is nonsensical to decrypt the message basing the cypher text and knowledge of encryption/decryption algorithm

However, there are some issues with it:

* The number of keys that have to be shared
* Concept of digital signature

**Asymmetric Key cryptosystem**

Public-key cryptography or asymmetric key cryptosystem is a class of algorithms, which need two keys: one is secret and the other is public they are mathematically linked. The public key is utilised for verifying digital signatures or encrypt the plaintext. The other is key is used for decrypting or creating a digital signature. (Zele & Vidya, 2014)14

### Steganography

Steganography is a technique that helps to hide the actual message, using other messages as a cover. Years ago, people tended to use invisible ink, tiny pin punctures on specific characters, and almost non-existent changes to handwriting.

In the modern age, the last 2 bits are encrypted by using a picture. In other words, the sender finds the last 2 bits and replaces them with a picture. (Zele & Vidya, 2014)14

Conclusion

To finish off, from my report you can now understand the value of network security for a better online experience. It also gave me the insight into the possible ways we can counterattack the hacker, but also the problems with the current technologies that we use to protect ourselves and our information and the security in itself.