INTRODUCTION

Internet is among the most important inventions of the 21st century which have affected our life. Today internet have crosses every barrier and have changed the way we use to talk, play games, work, shop, make friends, listen music, see movies, order food, pay bill, greet your friend on his birthday/ anniversary, etc. You name it, and we have an app in place for that. It has facilitated our life by making it comfortable. Gone are the days when we have to stand ina long queue for paying our telephone and electricity bills. Now we can pay it at a click of a button from our home or office. The technology have reached to an extent that we don‟t even require a computer for using internet. Now we have internet enabled smartphone, palmtops, etc. through which we can remain connected to our friends, family and office 24x7. Not only internet has simplified our life but also it has brought many things within the reach of the middle class by making them cost effective. It was not long back, while making an ISD or even a STD call, the eyes were stricken on the pulse meter. The calls were very costly. ISD and STD were used to pass on urgent messages only and the rest of the routine communication was done using letters since it was a relatively very cheap. Now internet have made it possible to not only talk but use video conference using popular applications like skype, gtalk etc. at a very low price to a level where a one hour video chat using internet is cheaper that the cost of sending a one page document from Delhi to Bangalore using speed- post or courier service. Not only this, internet has changed the use of the typical devices that were used by us. Television can be used not only for watching popular tv shows and movies but can be used for calling/ video chatting with friend using internet. Mobile phone is not only used for making a call but viewing a latest movie. We can remain connected to everyone, no matter what our location is. Working parents from office can keep eye on their children at home and help them in their homework. A businessman can keep eye on his staff, office, shop, etc with a click of a button. It has facilitated our life in more than one way. Have you ever wondered from where this internet came? Let us discuss the brief history of internet and learn how this internet was invented and how it evolved to an extent that now we cannot thinkof our lives without it.

I don‟t know what the cold war between USA and Russia gave to the world, but defiantly the internet is one of those very useful inventions whose foundation was laid during cold war days. Russia Launched the world‟s first satellite, SPUTNIK into the space on 4th October, 1957. This was clearly the victory of Russia over the cyber space and as a counter step, Advanced Research Projects Agency, the research arm of Department of Defence, United States, declared the launch of ARPANET(Advanced Research Projects Agency NETwork) in early 1960‟s. This was an experimental network and was designed to keep the computers connected to the this network to communicate with each other even if any of the node, due to the bomb attack, fails to respond. The first message was sent over the ARPANET, a packing switching network, by Leonard Kleinrock's laboratory at University of California, Los Angeles (UCLA). You will be surprised to know that the fist message that was sent over internet was "LO". Actually they intended to send work "LOGIN" and only the first two letters reached its destination at second network node at Stanford Research Institute (SRI) andbefore the last three letters could reach the destination the network was down due to glitch. Soon the error was fixed and the message was resent and it

The major task that ARPANET have to play is to develop rules for communication i.e. protocols for communicating over ARPANET. The ARPANET in particular led to the development of protocols for internetworking, in which multiple separate networks could be joined into a network of networks. It resulted in the development if TCP/IP protocol suite, which specifies the rules for joining and communicating over APRANET.

Soon after, in 1986 NSF(national Science Foundation) backbone was created to and five US universities‟ computing centres were connected to form NSFnet. The participating Universities were:

- Princeton University -- John von Neumann National Supercomputer Center, JvNC
- Cornell University -- Cornell Theory Center, CTC
- University of Illinois at Urbana-Champaign -- National Center for Supercomputing Applications, NCSA
- Carnegie Mellon University -- Pittsburgh Supercomputer Center, PSC
- General Atomics -- San Diego Supercomputer Center, SDSC

NFSnet, the successor of ARPAnet, become popular by 1990 and ARPANET was decommissioned. There were many parallel networks developed by other Universities and other countries like United Kingdom. In 1965, National Physical Laboratory(NPL) proposed apacking switching network. Michigan Educational Research Information Triad formed MERIT network in 1966 which was funded and supported by State of Michigan and the

The major task that ARPANET have to play is to develop rules for communication i.e. protocols for communicating over ARPANET. The ARPANET in particular led to the development of protocols for internetworking, in which multiple separate networks could be joined into a network of networks. It resulted in the development if TCP/IP protocol suite, which specifies the rules for joining and communicating over APRANET.

Soon after, in 1986 NSF(national Science Foundation) backbone was created to and five US universities‟ computing centres were connected to form NSFnet. The participating Universities were:

- Princeton University -- John von Neumann National Supercomputer Center, JvNC
- Cornell University -- Cornell Theory Center, CTC
- University of Illinois at Urbana-Champaign -- National Center for Supercomputing Applications, NCSA
- Carnegie Mellon University -- Pittsburgh Supercomputer Center, PSC
- General Atomics -- San Diego Supercomputer Center, SDSC

NFSnet, the successor of ARPAnet, become popular by 1990 and ARPANET was decommissioned. There were many parallel networks developed by other Universities and other countries like United Kingdom. In 1965, National Physical Laboratory(NPL) proposed a packing switching network. Michigan Educational Research Information Triad formed MERIT network in 1966 which was funded and supported by State of Michigan and the National Science Foundation (NSF). France also developed a packet swiching network, know as CYCLADES in 1973.

Now there were many parallel systems working on different protocols and the scientist were looking for some common standard so that the networks could be interconnected. In 1978, TCP/IP protocol suits were ready and by 1983, the TCP/IP protocol were apopted by ARPANET.

In 1981, the integration of two large network took place. NFS developed Computer Science Network(CSNET) and was connected to ARPANET using TCP/IP protocol suite. Now the network was not only popular among the research community but the private played also took interest in the network. Initially NFS supported speed of 56 kbit/s. It was upgraded to 1.5 Mbit/s in 1988 to facilitate the growth of network by involving merit network, IBM, MCA and the state of Michigan.

After the copertates took realized the strength and merit of this network, they particepitaqted in the develoement of the network to ripe its benefits. By late 1980s many Internet Service Providers(ISPs) emerged to provide the backbone for carrying the network traffic. By 1991, NFSNET was expended and was upgraded to 45Mbit/s. Many commercial ISPs provided backbone serive and was popular among the corporate. To facilitate the commercial use of the

network, NFSNET was decommissioned in 1995 and now the Internet could carry commercial traffic.

Now more and more Universities and research centres throughout the world connected to it. Now this network was very popular amongs the research community and in 1991 National Research and Education Network (NREN) was founded and the World Wide Web wasreleased. Initially the role of internet was only limited to file transfer. The credit of internet what we see it today goes to Tim Berners-Lee who introduced www.With the advent of www, there was a transformation on how the network was used. Now this web of information can be used to retrieve any information available over the internet. Software called, browser was developed to browse the internet. It was developed by researchers at University of Illinois in 1992 and named as Mosaic. This browser enables to browse the internet the way we browse it today.

Internet Addresses

With so many devices connected to the internet, we require some mechanism to uniquely identify every device that is connected to the internet. Also we require some centralized system which takes care of this mechanism so that the signs which are used to identify each device are not duplicate; else the whole purpose is defeated. To take care of this, we have a centralized authority known as Internet Assigned Numbers Authority (IANA), which is responsible for assigning a unique number known as IP(Internet Protocol) address. An IP address is a 32-bit binary number which is divided into four octets and each octet consists of 8 binary digits and these octet are separated by a dot(.). An example of an IP address is

11110110.01011010.10011100.1111100

Each 8-bits in an octet can have two binary values i.e. 0 and 1. Therefore, each octet can have minimum value 0. i.e. 00000000 to maximum value 256 i.e. 11111111 and in total have 2^8= 256 different combinations.

Again to remember this 32-bit address in binary is bit difficult, so for the better understanding of the human being, it is expressed in a decimal format. But this decimal format is for human understanding only and the computer understands it in binary format only. In decimal, the above IP address is expressed as 123.45.78.125

These octets are used to create and separate different classes. An IP address consists of two parts viz. **Network** and **Host.** Network part identifies the network different network and the host part identifies a device of a particular network.

This address uniquely identifies a devices connected to the internet similar to the postal system where we identify any house by fist identifying the county, then state, district, post office, cluster/block and finally the house number. These IP addresses are classified into five categories based on the availability of IP range. These categories/classes are:

Table 1: IP Address Classes

Class	Address range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or Research and Development Purposes.

Each 8-bits in an octet can have two binary values i.e. 0 and 1. Therefore, each octet can have minimum value 0. i.e. 00000000 to maximum value 256 i.e. 11111111 and in total have 2^8= 256 different combinations.

Again to remember this 32-bit address in binary is bit difficult, so for the better understandingof the human being, it is expressed in a decimal format. But this decimal format is for human understanding only and the computer understands it in binary format only. In decimal, the above IP address is expressed as 123.45.78.125

- APNIC- This RIR is responsible for serving the Asia Pacific region
- AfriNIC- This RIR is responsible for serving the African region
- ARIN- This RIR is responsible for serving North America and several Caribbean and North Atlantic islands
- LACNIC- This RIR is responsible for serving Latin America and the Caribbean, and
- RIPE NCC- This RIR is responsible for serving Europe, the Middle East, and parts of Central Asia

DNS

Whenever we browse any website in the internet, we type name something likewww.uou.ac.in and we rarely deal with IP address like 104.28.2.92 but the fact is even if we type http:\\ 104.28.2.92 in the URL, it will land us to the same webpage. The fact is we are very comfortable using and remembering the names instead of a number. Moreover, these IP address changes over time and some of the sites have multiple IP address. Also, the transfer ofthe data over internet is only possible using IP addresses because the routing of the packet of data sent over internet is done using IP address. There is a server called Domain Name System(DNS) which take cares of this translation job to simplify and to save us from remembering these changing IP address numbers, the DNS. Whenever you type an address like http:\\www.uou.ac.in, there is a process called DNS name resolution, takes place in the background. The computer keeps the track of recently visited sites and locally maintains a database in DNS cache. In case, the IP address of the site you have requested for is not found in

the DNS cache of your local computer, then the next probable place to find it is DNS server of your Internet Service Provider(ISP). These DNS servers of ISP also maintain the cache of the recently visited pages. Just in case, the information is not found here also, the DNS server of the ISP forward the query to the root nameservers. The root name servers publish the root zone file to other DNS servers and clients on the Internet. The root zone file describes where the authoritative servers for the DNS top-level domains (TLD) are located. There are currently 13 rootname servers. They are:

- A - VeriSign Global Registry Services

Before discussing the matter further, let us know what the cyber crime is?

The term **cyber crime** is used to describe a unlawful activity in which computer or computing devices such as smartphones, tablets, Personal Digital Assistants(PDAs), etc. which are stand alone or a part of a network are used as a tool or/and target of criminal acitivity.

Classification of Cyber Crimes

The cyber criminal could be internal or external to the organization facing the cyber attack. Based on this fact, the cyber crime could be categorized into two types:

- *Insider Attack:* An attack to the network or the computer system by some person with authorized system access is known as insider attack. It is generally performed by dissatisfied or unhappy inside employees or contractors. The motive of the insider attack could be revenge or greed. It is comparitively easy for an insider to perform a cyber attack as he is well aware of the policies, processes, IT architecture and wealness of the security system. Moreover, the attacker have an access to the network. Therefore it is comparatively easy for a insider attacker to steel sensitive information, crash the network, etc. In most of the cases the reason for insider attack is when a employee is fired or assigned new roles in an organization, and the role is not reflected in the IT policies. This opens a vernability window for the attacker. The insider attack could be prevented by planning and installing an Internal intrusion detection systems (IDS) in the organization.
- *External Attack:* When the attacker is either hired by an insider or an external entity to the organization, it is known as external attack. The organization which is a victim of cyber attack not only faces financial loss but also the loss of reputation. Since the attacker is external to the organization, so these attackers usually scan and gathering information.An expreicend network/security administrator keeps regual eye on the log generated by the firewalls as extertnal attacks can be traced out by carefully analysinig these firewall logs. Also, Intrusion Detection Systems are installed to keep an eye on external attacks.

The cyber attacks can also be classified as structure attacks and unstructured attacks based on the level of maturity of the attacker. Some of the authors have classified these attacks as a form of external attacks but there is precedence of the cases when a structured attack was performed by an internal employee. This happens in the case when the competitor company wants the future strategy of an organization on certain points. The attacker may strategically gain access to the company as an employee and access the required information.

Unstructured attacks: These attacks are generally performed by amatures who don‟t have any predefined motives to perform the cyber attack. Usually these amatures try to test a tool readily available over the internet on the network of a random company.

Structure Attack: These types of attacks are performed by highly skilled and experienced people and the motives of these attacks are clear in their mind. They have access to sophisticated tools and technologies to gain access to other networks without being noticed by their Intrusion Detection Systems(IDSs). Moreover, these attacker have the necessary expertise to develop or modify the existing tools to satisfy their purpose. These types of attacks are usually performed by professional criminals, by a country on other rival countries, politicians to damage the image of the rival person or the country, terrorists, rival companies, etc.

Cyber crimes have turned out to be a low-investment, low-risk business with huge returns. Now-a-days these structured crimes are performed are highly organized. There is a perfect hierarchical organizational setup like formal organizations and some of them have reached a level in technical capabilities at par with those of developed nation. They are targeting large financial organizations, defence and nuclear establishments and they are also into online drugs trading.

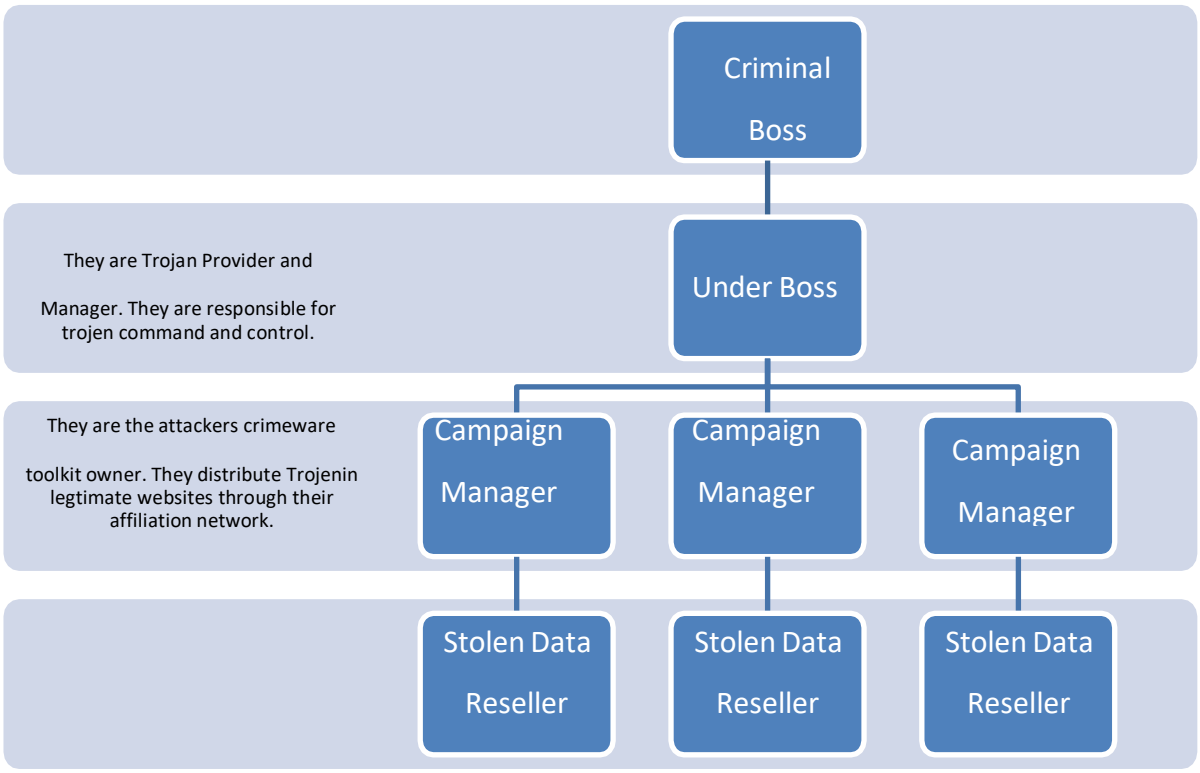

Figure 1 : Hierarchical Organisational Structure

- B - University of Southern California - Information Sciences Institute
- C - Cogent Communications
- D - University of Maryland
- E - NASA Ames Research Center
- F - Internet Systems Consortium, Inc.
- G - U.S. DOD Network Information Center
- H - U.S. Army Research Lab
- I - Autonomica/NORDUnet
- J - VeriSign Global Registry Services
- K - RIPE NCC
- L - ICANN
- M - WIDE Project

These root nameservers directs the query to the appropriate Top-Level Domain(TLD) nameservers by reading the last part of the URL first. In our example the url was http:\\www.uou.ac.in. The last part is .in. Some of the examples of TLD name servers are .com, .biz, .org, .us, .in, etc. These TLD nameservers acts as a switchboard and direct the query to the appropriate authoritative nameserver maintained by each domain. These authoritative nameserver maintains DNS records along with other useful information. This address record is returned back to the requesting host computer via TLD nameservers, nameservers, ISP‟s DNS

server. These intermediaty server keeps the recond of this IP addressin their DNS cache, so that if the same request is encountered again , they don‟t have to go through this process again. If the same URL is requested again, the DNS cache of the local host computer will return the IP address of the URL.

Internet Infrastructure

Internet, as the name suggests, in a network of network i.e. it is a collection of several small, medium and large networks. This clearly indicates to one fact, nobody is a single owner of the internet and it is one of the proven example of collaborative success. Now you must be surprised how such a large network which is spread across the continents can run without the any problem. Yes it is correct that to monitor such a large network, we require an international body which can frame the rules, regulation and protocols to join and use this network. Therefore, an international organization, known as "The Internet Society" was formed in 1992 to take care of such issues.

Let us now discuss, how this internet works? How the email you sent to your friend is received by your friend‟s computer located at another country/continent. When you areworking in your laptop/desktop in your home without connecting to the internet, your computer is a standalone system. But, whenever you connect to the internet by dialling to your Internet Service Provider(ISP) using your modem, you become the part of the network. The ISP is the link between the internet backbone, through which the entire data route, and the user. The ISP connects to the internet backbone at Network Access Points(NAP). These NAPs are the provided by the large telecommunication companies at various regions. These large telecommunication companies connect the countries and the continents by building and maintaining the large backbone infrastructure to route data from NAP to NAP. ISPs are connected to this backbone at NAP and are responsible build and manage network locally. So when you dial internet through modem, you first become part of the local ISP, which in turn connects to the internet backbone through NAP. The data is routed through this backbone and sent to the destination NAP, where the ISP of your friend‟s network is located. As soon as your friend dials his modem to connect to the internet, the data is delivered to your friend‟s computer.

World Wide Web

Sometimes we interchangeably use the term internet and world wide web or simply the web, as it is popularly known as. But web is only one of the several the utilities that internet provides. Some of the popular service that internet provides other then web is e-mail, usenet, messaging service, FTP, etc. The web use HTTP protocol to communicate over internet and to exchange information. The web was developed at CERN (Europeen de Reserches Nucleaires), Switzerland) by a UK scientist Tim Berners-Lee in 1989. It consists of all the public web sites and all the devices that access the web content. WWW is an information sharing model which is developed

to exchange information over the internet. There are plenty of public websites, which is a collection of web pages, available over the internet. These web-pages contain plenty of information in a form of text, videos, audio and picture format. These web pages are access using a application software called a web browser. Some of the examples of the popular web browser are: Internet explorer, Chrome, Safari, Firefox, etc.,

So this was a little indroduction about internet and how it functions. Now let us discuss about cyber crime