Chapter 1

Introduction

1.1 Background and Introduction

Security in general is the state of being secure or simply it's the protection from any damage to any valuable or vulnerable asset that one possesses. Just like the human race, which has come a long way, right from the Stone Age, to the current age of Information and Communications Technology, security has also progressed and changed its meaning and form with the changing times. From the cave-man of Stone Age, for whom security just meant protecting himself from other living creatures (using a club as his weapon) to the 21^{ist} Century, where security is mostly concerned with how well you can protect your Information Resources. (This includes everything from providing physical security to the Information Systems to restricting access to authorised persons and protecting it from any malicious or unauthorised use and access). The primary Information Resource is a Computer. But a standalone Computer or an Information System is not of much use unless it is connected to a Network or simply to Internet, both of which offer services like remote access to Information and sharing of Information and other resources. Internet is the backbone of current age of Information and Communications Technology. From an individual to a Private Enterprise or any other Organization people are making heavy use of this technology on a daily basis. The rapid growth of Computers together with communication technologies has added fuel to the fire, it has changed the way in which people look at information processing and communication and thus has influenced the way Enterprises, Government bodies and others function in today's world [1, 2, and 3]. It has revolutionized everything in the field of business, banking, education, defence, research, health-care, etc. Internet as you know is a world-wide collection of interconnected networks that are accessed by remote hosts in a number of ways. Anyone with a Computer, Laptop, Smart Phone or any other hand-held device and a Data Connection can have access to Internet and thus to the Global Information resources which it provides. The Organizations (public/private enterprises, government bodies and others) can access and share Information across the Globe with ease and within no time.

Before the dawn of Internet the goal of the Internet stakeholders was to provide an open network, meant for researchers to share their new discoveries and research

resources. Second was to provide a mechanism for military groups for exchange of Information [4]. The main design priority was openness and growth of the network while as security issues were of less concern. The first major security incident on the internet was the occurrence of the Morris Worm [5] in 1988. While as the first PC virus reported was BRAIN [74] in 1986. However, during those days the Internet was not as popular as it now, therefore the world which had just seen the dawn of the Internet certainly did not show any dependence on the Internet as the world is showing now and was still limited to chosen organizations like military, research and educational organizations until the mid-1990s. This is the reason why there was not much attention given to Security in the Internet. In US the Internet was fully commercialized during mid-1990s but it had already begun to spread rapidly in Europe and Australia in late 1980s and Asia in early 1990s [6].

With the rapid growth and success of Internet in the last two decades, the Internet has become a game changer in almost every field and has significantly changed its traditional role. With the changing times it has no longer remained just a tool for the researchers or the communicators. Governments are using Internet in *e-Governance* and in number of ways to provide information to the citizens of a nation or to the World at large and this trend is a successful one [7] and as expected Governments in future will continue the use of Internet to provide better and transparent governance. Enterprises use Internet for *e-Commerce,* information exchange with business units, partners, suppliers and customers in a very efficient and smooth manner. Research and Educational Institutions use Internet as a tool for assisting in problem solving, as a platform for collaboration and spreading their Discoveries and Inventions all over the world. Now with such use it is evident that organizations are becoming more and more dependent upon Internet and network based Information Systems. Because of its wider reach and its ease it has given them the possibility of growing at a rapid pace [7, 8, 9 and 10]. Now with such ease of access and dependence upon Information and Information Resources, the Organizations are exposed to great risk [11], if the access to an Information System is disrupted, manipulated or destructed. The risks are that the valuable Information will be lost, stolen, changed or misused. Unfortunately with the

good i.e. Growth of the Internet, came the bad i.e. The Attacks, they have also progressed and increased at a parallel rate.

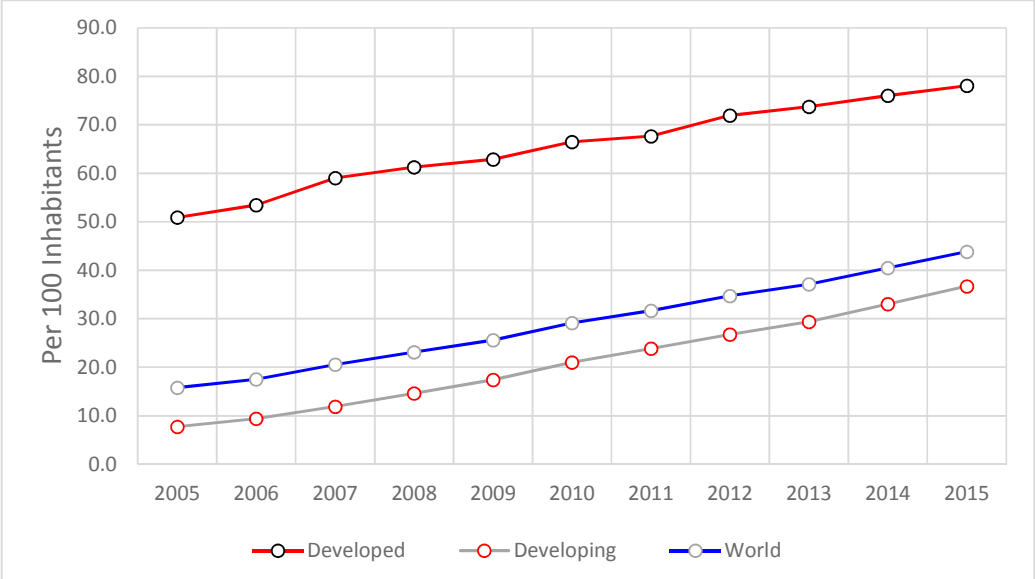

Figure 1.1: Internet users per 100 inhabitants, world-wide 2005-2015.

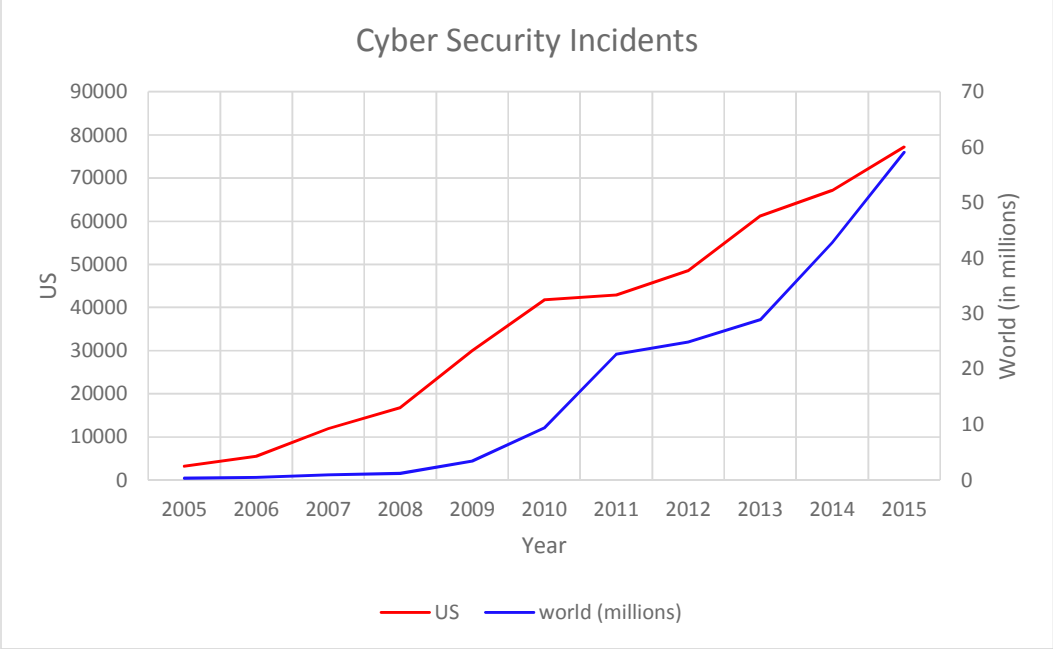

Figure 1.2: Growing number of Cyber Security incidents reported in US and Worldwide.

Figure 1.1[1] shows the use of internet in the last ten years. As expected the graph complements the fact that Internet has grown consistently every year. Now in comparison to this graph, Figure 1.2[2], a study carried out by United States Government [12] shows that the growth in cyber security incidents from 2005-2015 in United States, country with maximum number of Internet users[1] . Both the figures and some data from [14] prove the fact, that with the growth of the Internet, the attacks have also increased significantly.

An important situation here is, nation's essential services such as, banking system, transportation, power, healthcare, and defence, their conventional way of operations are being replaced on a step-by-step basis by cheaper, more efficient Internet and Network based applications. Historically speaking whenever a nation has attacked any other nation, it is always seen as an attack on a nation's critical services and for that matter the attacking nation has to cross into the physical boundaries of the victim nation. An action of this sort can be blocked and averted by a nation's security services. However the connectivity of nation's globally through Internet makes the physical boundaries look meaningless to a large extent, as Internet based attacks can be launched from anywhere in the world to disrupt these critical resources.

Some attacks can also bring huge physical destruction to a nation in today's world, because some critical energy resources and nuclear resources are also network controlled in today's world of Science and Information Technology. Although the nuclear arsenal of a nation is under heavy security cover, usually the most secure location in the nation or *Security by Obscurity* [15], but still there have been attacks on such facilities, like recently in 2010 the attack on IRAN's Nuclear facility by a virus named as *STUXNET* [16], more of a cyber-weapon with serious physical consequences than just a virus. Unfortunately no Internet based service or any computer or a network is immune from Cyber-attacks, because most of these attacks are based on using ordinary protocols and exploiting the security holes in victims OS or on the network devices . This is the reason why security researches and practitioners are of the opinion that, no system is 100% secure and we can only mitigate attacks, but no remedy for

[1] Source: ITU World Telecommunication / ICT Indicators database

[2] Source: GAO analysis of US-CERT data and cyber security incidents worldwide from statista.com

removing them completely. Therefore, the *Security* of the Internet is not confined to information sharing and online businesses only, but it is a serious issue of national security and should be dealt with importance. Since Internet is actually the main information resource and everything revolves around the *Information* i.e. Information creation, processing, access, transmission, reception etc. No matter which application or service we are using on Internet we are always doing one of the above things with the *Information.* Given the risks and attacks to Internet, Information Systems or any other information resource a user always expects certain assurances before indulging into serious use of the same. The User expects the following things:

1. The Information used is reliable and coming from a trusted and known source. If the source is unknown, there should be enough mechanisms in place to prove that the source is not a malicious one.
2. The Information and related resources are available and accessible, whenever they are needed.
3. Information processing and sharing will be dealt only in the manner which they know and which they expect. Any unexpected situation may be a threat.
4. The information processing systems in use will process Information in a timely and reliable manner.

In other words we can simply say that the Information and the Global Information Infrastructure which are being thoroughly used by business community, government organizations and normal home users, should be free from any risk, unauthorised use, vulnerability or attacks and the service providers should deliver services to the End-User as promised or if there is a contract signed, then as documented in the *Service Level Agreement (SLA)*. In simpler words users of these resources want to be assured of the Security of Information.

1.2 Overview of Denial of Service Attacks

Denial of Service Attack has proven to be the most dangerous, damaging and a threat that can be a never ending one to the users, organizations and to the global infrastructure of the Internet [17]. The goal of this attack is to prevent access either to an online service like a web-server, the victim's network or simply damaging the Host machine of the user [18] i.e. A DoS attack exhausts a web-server's resources like disk space or CPU time for computation of response or the network bandwidth, so that the web-server is prevented from providing service to its legitimate users. DoS attack may even bring down the host machine by simply exploiting some software bug in the Operating System and thus ceasing all the ways for the user to access any resource. Another form of this attack which is more lethal and destructive because of its distributed nature, is *Distributed Denial-of-Service (DDoS)* attack, in which a single victim is attacked by a large number of compromised hosts, which are geographically distributed over the Internet. Just like a simple DoS attack, this attack can also crash the victim or it may keep the victim busy handling the *Attack Traffic* and thus keeps the legitimate users at bay. The legitimate users may have to wait for the victim's service as long as the attack traffic is there or in worst cases, if the attack persists for longer time the Users may get no service at all until the victim's service is freed from such an attack. The attackers often carry out these type of attacks by using false identities to prevent themselves from being caught in case of an early detection. Both forms of attacks make use of vulnerabilities in end-user systems, networking devices like routers, and other systems connected to a computer network or Internet.

The main reason that makes DoS attacks attractive and easy to carry out for the attackers is that there are enough automatic tools available to carry out these attacks [18, 19, and 20]. Without any expert knowledge one can easily carry out these attacks using these tools. One more reason for the popularity and the easy life of DoS attacks on the Internet is that the Internet was not planned for such problems. To address this problem from the root cause we need to re-design everything from the scratch while keeping in view all the security aspects that are necessary for the secure infrastructure of the Internet. Now this is clearly not and easy job to carry out given the cost and complexity that will be associated with it. Therefore one cannot address this problem

from the root cause, we can only find a solution that fits in the current architecture and certainly this solution will involve trade-offs [21] on both security and performance, no matter how efficient the solution may be. Another reason for weak security is the cost, more the security more will be the cost.

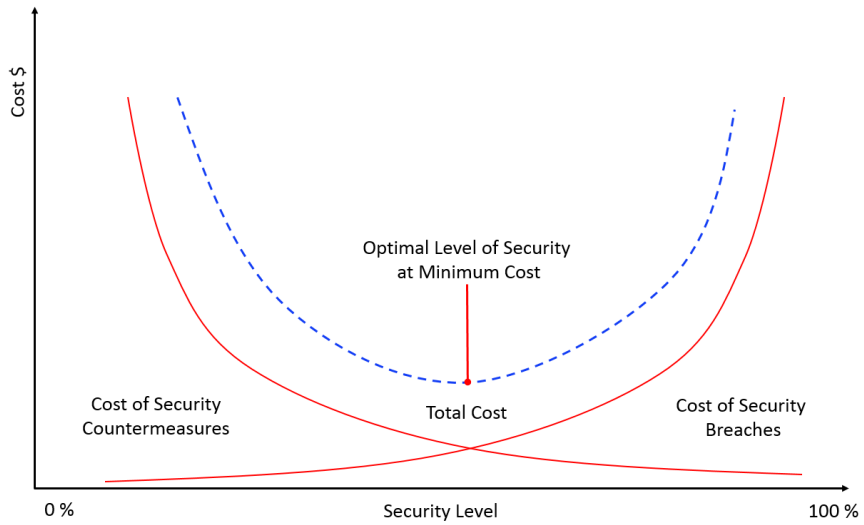

Figure 1.3: Security level and Cost.[3]

The best way to tackle such an issue is an optimal level of security at an optimal cost, as shown in figure 1.3.Therefore in the present architecture of Internet it is difficult to keep the DoS attacks at bay.

1.2.1 DoS Attacks in Real World

During the last decade and a half, since the occurrence of the first DoS attack [22], they have grown in stature significantly. A DDoS attack under 10Gbps is too mainstream these days. DDoS attack reported a decade ago attacked at the rate of 8Gbps-this year the attack rate has increased exceptionally. The largest attack reported last in 2016, 2015 and 2014 was 600, 500 and 400 Gbps respectively [23] as reported by ARBOR Networks[4]. An analysis of the peak DDoS attacks in the period 2004-2016 is shown in

[3] Internet Security Alliance July 2002, Data from Dr. William M. Hancock, Exodus, A Cable and Wireless Service.

[4,5] Arbor Networks is a company which specializes in DDoS attack Defence , the data has been collected from 287 Service providers worldwide.

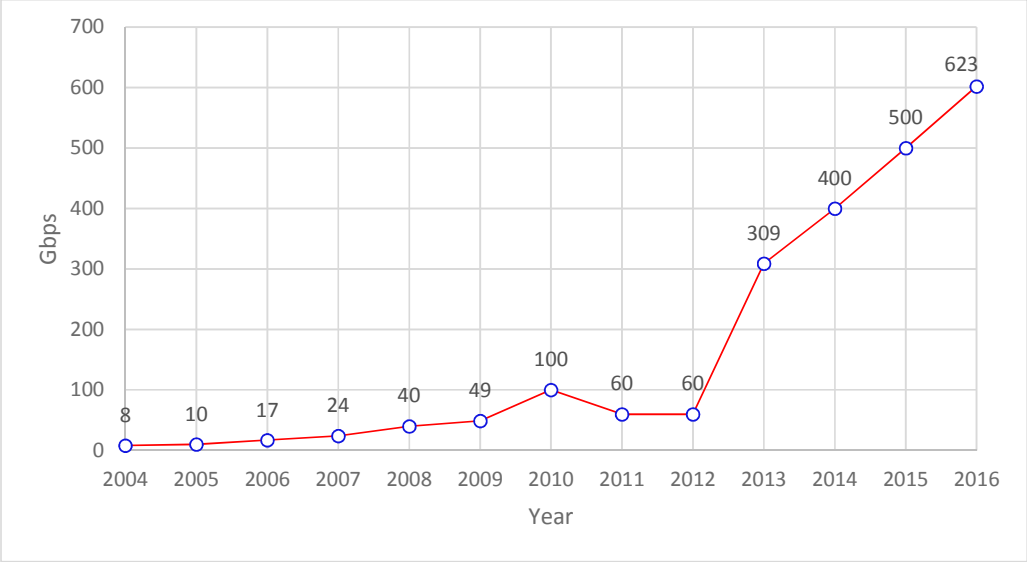

Figure1.4: Peak Attack Size in the past decade[5].

the figure 1.4[6]. Some other attacks that were reported in the same report were of the rates of 300 Gbps, 200 Gbps and 170 Gbps and there are six more that crossed the 100 Gbps threshold. The reasons for the attacks lately have been nihilism, vandalism, online gaming and ideological hacktivism [23]. Some of the high profile Denial of Service attacks that made news during 2010-2015 are discussed in this section.

The year 2015 started with an attack in France on satirical newspaper Charlie Hebdo, who had published and shown disrespect to the Prophet Muhammad (PBUH). In wake of this attack 19,000 French websites were hit by DDoS [24]. In the same month i.e. January, Extra-torrent was also DDoS attacked [25]; website was down for 23 hours.

The year 2014 ended with a DDoS attack of huge rate at around 25 Gbps on a Domain Name Service provider DNSimple and about 50 million packets were being sent per second [26].The same month a famous hacker group named Lizard Squad attacked Xbox Live PlayStation Network [27, 28] twice in a span of 8 days. In the same month Sweden's fixed line broadband network was a victim of collateral damage as a

[5] Source Arbor Networks, Inc.

result of a DDoS attack on a mystery gaming site [29]. Telia the Sweden's Broadband giant was again attacked courtesy of the fact that Telia was closely linked to a police raid on the Pirate Bay [30] and experts say this provoked feelings in the hacker community and they believe the group behind this attack was the Lizard Group. In the month of November Supreme Court of Canada and Ottawa Police Services went down due to DDoS attack [31]. On November 22, the hacker group Anonymous declared 22 November as "International day against Police violence" and took down several police websites in Italy [32]. The next day EA Games online service brought down by the hacker group Lizard Squad [33]. In the month of October the hacker group Anonymous took down top 43 Israeli Government websites against the killing of a 12 year old U.S. citizen [34]. September saw a group of hackers "Anonymous Op Pakistan," make a bid to remove "every vestige of the Pakistan government from the Internet" [35]. In the month of August hackers from the group Anonymous took down some important Israeli government websites in wake of shutdown of twitter accounts of the group [36]. In the month of July Anonymous hackers take down Mossad website in wake of Gaza attacks [37]. In June Evernote was DDoS attacked and the outage affected millions of users who were unable to sync their notes and web clippings [38]. In May Domain name hosts "Point DNS," was hammered by a high intensity DDoS attack, knocking out the servers for hours [39]. In the month of March GitHub fell prey to the hands of DDoS attack twice but GitHub has a defence mechanism in place against such attacks, so the server was up and running some minimal downtime [40, 41]. The month of February witnessed the largest ever DDoS attack in the history of the attack. A client of the content delivery network Cloudfare was DDoS attacked and the volume of the attack exceeded 400 Gbps, making it the largest DDOS attack ever recorded [42] then. The attack used Network Time Protocol (NTP) reflection. In the same month Bitcoin was attacked by unknown hackers. This attack halted the working of two Bitcoin exchanges [43].

The month of December in 2013, witnessed lots of DDoS attacks on various gaming sites and servers [44]. In the month of November the Battlefield 4-PC servers were DDoS attacked thus leaving an army of virtual soldiers unable to compete [45]. In the month of September the Loose-knit hacker group posted on Pastebin about a DDoS attack that brought down Japanese Microsoft websites and servers [46]. June saw some

attacks on DNS service providers [47, 48]. In May some Government sites in Saudi Arabia were attacked by the group Anonymous [49]. April and January witnessed a lot of DDoS attacks by different groups on many banks in different countries [50, 51]. April also witnessed an attack on the download infrastructure of VideoLAN. The outage lasted for 30 hours [52].

In October of 2012 GitHub was again at centre stage of DDoS attacks, was attacked twice in October and the attacks on banks continued this month also and certain Government websites were also taken down [53]. September saw some of the sites of the Attorney General of Australia being attacked courtesy of the Operation Free Assainge [54]. In May an Anonymous hater takes down WikiLeaks for 72 hours and also The Pirate Bay [55]. In April some domains belonging to NASA were taken down courtesy of the occurrence of OPTrailAtHome and Navittaja and in the same month Anonymous attacks Formula 1 websites in the name of #OpBahrain [56].

In November of 2011 Internet services in Gaza and West Bank were attacked after Palestine won a Symbolically Significant victory at UNESCO [57]. July saw some attacks on some Universities in Italy [58]. In July Anonymous took down 74 Turkish websites releasing a repository of Government data which would have been harvested from more than 100 Turkish Government Domains [58]. In June Spanish police websites taken down by Anonymous [59] and also in the same month LulzSec brings down the public CIA website [59].

December of 2010 saw an attack on MasterCard, PayPal, Visa and PostFinance. Attack was launched in support of WikiLeaks and lasted more than16 hours. In November an attack of the magnitude 10 Gbps was launched on WikiLeaks to prevent the release of secret cables [60].

This study on the DoS attacks in the recent years tells us that these attacks are growing at par with the changing technology, the sophistication levels and the new tactics used to attack. If the problem is not taken care of very quickly, the loss it can incur will be huge which can often result in serious consequences. Therefore the solution should be the other way round i.e. the technology used and the mitigation techniques used to curb such attacks should be way ahead in every aspect, to that of the hackers.

1.3 Security Nomenclature and Basic Concepts

This section defines and gives brief explanation of most important terms used in describing the Security paradigm related to Information, Computers and Networks. The terminology will be used throughout the thesis.

1.3.1 General Security Terminology

The theme of the thesis revolves round the security of information i.e. *Information Security,* which can't be safeguarded unless the issues and risks related to both *Computer Security* and *Network Security* are addressed in a proper way. Starting with the absolute basic, the definition of the term *Security* used in the thesis, which is based on the ideas from [61, 62, 63 and 64].

We define *Security* as a Continuous Process towards an acceptable level of resistance against any known risks**.** A risk can be intentional or an unintentional one [61 and 65].

We define *Information Security* as an endless process towards an acceptable level of protection of Information from unauthorized access, leak, transfer, destruction, modification, handling or control [61and 65]. It may be noted that Information Security does not only deal with information being processed and stored in electronic form only. But the focus of this thesis is only on the Information being stored, processed and communicated electronically.

The definition of *Computer Security* is based on [62]. Computer Security is an endless process towards an acceptable level of prevention and detection of wrongful and unauthorized actions by users of a computer system. Any computer or an information system should have the necessary mechanisms to safeguard information, its processing, distribution and storage.

Almost all of the computers are connected to networks and most of them to Internet, therefore information access, transmission and reception is done remotely. For the smooth and risk free functioning we need *Network Security.* It is an endless process towards an acceptable level of safeguarding the network components, The Information over it, the connections and every other resource that is associated with information processing over the networks [66]. Over the period of time the gap between computer security and network security has been bridged as most of the computers or hosts are

connected to networks one way or the other and remotely any host can be accessed through the network just like we do when we are physically In-front of the computer [63].

The Fight against DoS or DDoS attacks is mostly network security as most of these attacks are launched and carried out remotely, as both the attacker and the victim are connected to the network.

1.3.2 Information Security Goals and Concepts

From the dawn of Information Security, to this time when it is the need of the hour and a critical factor for the smooth and positive business continuity, government and other organizational work, Information Security has surely come a long way. Security professionals have left no stone unturned and developed many protocols, tools and techniques in order to achieve three generally accepted information security attributes CONFIDENTIALITY, INTEGRITY, and AVAILABILITY [62, 65, 67 and 68].

Confidentiality is restricting unauthorized users, processes or entities from accessing the information which is intended for an authorized and a legitimate user [64]. When an unauthorized access, disclosure or any act of breaking of that sort happens to Information, it results in the loss of confidentiality.

Integrity is guarding against unauthorized and improper Information alteration, deletion, or loss. If Information is modified, altered or deleted in unknown ways, then the result is the loss of integrity.

Availability is ensuring access to information is done in a timely and reliable manner, whenever and wherever needed or in other words a system or a system resource is reachable and usable whenever and wherever requested by an authorized party, in accordance with the performance blueprint of the system [64]. It is as important as Confidentiality and Integrity. If Information becomes inaccessible or is not delivered on time, then it will result in loss of Availability. Good performance of availability is not possible without a reliable system, most importantly in environments such as intensive healthcare, aviation and traffic signalling.

The legitimate users of information who can be trusted with, to legitimize them we need *Authentication* and *Authorization.* Authentication is validating both the parties involved in a transaction or a communication, who they claim they are. The proof may

be, a user may have a password or the use of biometrics such as users fingerprint scan. Authorization is the process of finding out whether a particular user (or a process or a computer system) is allowed to carry out a certain action, such as accessing a file or executing a program or process [69], only authorized users are allowed to do so.

In a highly secure environment the means of authentication cannot be falsified i.e. *Non Repudiation* - a user of an information system or a transaction cannot later deny having received information nor can the other user deny having sent information [69].

A more general term that incorporates information security attributes and plus some other attributes of security goes by the name of *Dependability*. It is a general term used to describe the combination of *Confidentiality, Integrity, Availability, Reliability, Safety* and *Maintainability* [70]. *Dependability* is defined as the capability of a computer system to deliver service that can rightly be trusted [70].

1.3.3 Denial of Service Terminology

Denial of Service is forestalling the legitimate users of a resource from accessing the resource or simply creating a delay in the operations which are time-critical [62].The resources here are disk space, CPU time, the network bandwidth, memory and other structures like static memory [71].

Denial of Service Attack is a malicious attempt to disrupt, degrade or prevent the availability of an Information resource to the legitimate users. DoS attacks are intentional almost all of the times but sometimes unintentional human errors during the designing process or programming, can lead to DoS attacks [72]. The DoS attack that completely prevents the availability of a resource is called as the *Destructive DoS attack*. While as if the attack is only successful in bringing down the performance of the resource, it's called as a *Degradative (non-destructive) DoS attack*.

A DoS attack can be executed either as a *logic attack* or as a *flooding attack* [73]. A Logic DoS attack is based on exploiting vulnerability or a security hole in the target system. For example in the Internet Protocol (IP) packet, the Pay Load data size can be modified which may crash an operating system, due to a fault in the OS software. A flooding DoS attack on the other hand employs brute force. Legitimate looking but unwanted traffic is sent in huge volumes towards the victim. This results in resources being wasted on illegitimate and false requests. Network bandwidth, data structures like

memory allocations are filled with fake data, processing power is wasted on handling of fake requests. Today these kinds of attacks can be amplified and attacks can be executed and run in a coordinated fashion from multiple sources all over the globe.

An attack of this nature is called as *Distributed denial of service attack (DDoS),* which is defined as a deliberate and malicious attempt to disrupt, degrade or prevent the availability of an Information resource to the legitimate users by using attack traffic from multiple sources collectively at the time of the attack. The attack traffic usually comes from compromised hosts. These compromised hosts have a hierarchy, the bad guy better known as the Attacker controls the *Masters* (also known as handlers), which in turn control a much bigger in number, an army of *Agents*(also known as zombies or daemons). The Agents are handled by masters and masters are handled by the attacker himself to carry out an attack of distributed nature against the victim.

Master (or handler) is *a* compromised host whose job is to handle and control the working of a large set of agents.

Agent (or zombies or daemons or bots) is a compromised host whose job is to send attack traffic towards the victim during the DoS attack.

A network of this sophistication which contains masters and agents organised in a structured way i.e. hierarchically, and the main controller the attacker is referred to as the *DDoS network* or a *Botnet*.

Throughout the course of this thesis DDoS attack would be treated as a subsidiary of DoS attack and DoS attack would be used in general for describing the single source DoS attack and the multiple source DDoS attack.

1.4 Research Motivation

With the growth of computers and the Internet, Information processing became highly dependent on these two things. No doubt information processing became much easier, prospered and it also helped Organizations grow at a rapid pace, but with such ease of access and dependence upon Information resources came the risks. Information Security ensures that the risks are kept at bay or are handled properly so that information processing is done in a trustable, smooth and a reliable manner. Information security as we know consists of three basic principles i.e. Confidentiality, Integrity and

Availability. Over the past few decades Availability has not received much attention as Confidentiality and Integrity have and it remains the least explored and the most neglected attribute of security [75] and remains the same today as well [76]. While addressing the security issues it is not given much importance as the other two are given. Confidentiality and Integrity are dependent on Availability. If Information becomes inaccessible or is not delivered on time, then it will result in loss of Availability and loss of Availability means no access to information resource and that in-turn means one cannot address the issues of Confidentiality and Integrity, thus meaning that the information is not secure. So if Information Security has to hold we have to take care of Availability much more efficiently than Confidentiality and Integrity, it is the most critical attribute of Information Security. The main threat that Availability has is DOS attack. DoS attacks can render services unavailable or can slow down time critical services in order to affect the Availability of resources to legitimate users. Determining the key factors on which Availability is dependent and finding out how those factors are affected by DoS attacks, can help us analyse how Availability can be rendered ineffective by DoS attacks. This will help us study the problem in detail and would help in determining the solution of the problem right from the root cause.

As we know Internet was designed and developed around the idea of functionality i.e. How to move data packets from one device (*source*) to another (*destination*). The main priorities were openness with other systems and growth. Security was no issue initially, but as the Internet grew, security came into the picture and it was incorporated into the existing Internet Infrastructure. This design of internet obeys the *end-to-end paradigm*: sender initiates the communication process towards the destination. The network in-between does packet forwarding using an efficient routing algorithm. To enforce the desired level of service guarantees such as reliability, availability or other security attributes, the work is left to the advanced protocols at the sender and receiver with some help from the intermediate network nodes. The work of the intermediate network is simple and is optimized for packet forwarding and delivery while as the work of the end hosts are much more complex in this end-to-end paradigm [78]. If in the two way communication one of the parties decides to let loose and do some damage to the other party, the intermediate network intervenes and helps in handling such an attack. The attack here that we are talking about is DoS attack. Such

a design of internet provides many opportunities for DoS attackers and thus presents many challenges for the Security Community.

Mitigation of DoS attacks in general is divided into 4 stages: (i) attack prevention; (ii) detection; (iii) source identification; (iv) reaction (work in the thesis only focuses on the first part i.e. Attack prevention). A lot has been done to mitigate the problem of DoS attacks, still the problem exists today, reason being the internet design and the hardships faced in mitigating DoS attacks. Some of them are;

- Software bugs, communicating systems/devices or programs not being configured properly, the built-in nature of the human beings being vulnerable to social engineering [77] and various other factors, encourage and empower the attacker to render a resource unavailable. A large number of DoS attacks make use of above and exploit them to a desired level where they can orchestrate the attack.
- Sending attack packets with some sort of legitimacy is easy and almost free of cost, but it's not that easy to have a silver-bullet that can take down the illegitimate packets. Even if we have a fool proof mechanism to filter out such illegitimate packets, the filtering process can itself keep the router busy filtering the illegitimate and the legitimate packets, and if the packets are in huge number (like in DDoS), it may create a huge delay in packet arrival the destination or in worst case the processing capacity of the router may cease down and hence the result a DoS attack.
- To find the attacker it can take ages as one doesn't know how many layers of zombies are there and very easy for the attacker to remain hidden behind an army of zombies. In order to be affective, the Defense mechanism needs to find the source of the attack as soon as possible and this way serious damage can be averted
- The amount of work that has been done to compare, contrast and categorise various ideas and concepts related to DoS attacks and defense mechanisms is fair, but needs to be revisited every now and then because with the changing technology paradigm, new attacks are born and they also need to be handled before they create havoc. Also some attack programs might be redesigned in

order to bypass any security mechanism that was originally rendering the attack as ineffective; we need to keep track of this as well.

- Most of the Internet resources (server, network or any service) are limited in nature. Internet as you know is based on the concept of resource sharing, so these limited number of resources may get easily eaten up by enormous amount of users.
- Distributed control of the internet make is even worse. Each network across different countries is run and governed by local policies defined by the stakeholders present in the respective regions. There needs to be a global security policy and security mechanism. But this thing is impossible in practice as there are different privacy concerns across countries. DDoS attacks most of the times generate cross-network traffic. If an attack of this sort is detected it is even more difficult for the security people to investigate because of the distributed control thing.

1.5 Research Objectives

The main motif of the thesis is *"how can we ensure Information Availability or Availability of an Information System or Availability of a Network based resource, to the legitimate user of that Information resource by Preventing Denial of Service Attacks,"* in such a way that the solution to the problem is found within the current information architecture paradigm. The paradigm includes everything from Information processing on an information system to how we communicate that information to connected hosts through the use of computer networks. In support of above the aim of the research is:

1. A detailed study on *Availability* as a security attribute and identifying the factors that determine the Availability of Information or an Information System. Factors identified at:
    a) System level.
    b) Component level.
2. Analysis of the identified factors and a detailed study on the impact of these factors on Availability:

2.1 Analyze the identified factors of system level against DOS attacks and a detailed study on the effect DoS attacks can have on the Availability on an Information System.

2.2 Design and evaluate a security measurement system for security analysis beyond the system level i.e. Design, evaluation and analysis of a component level metric. Evaluation done on a system with a CBD system architecture.

3. A detailed study on how DoS attacks are orchestrated and an analysis of most frequently occurring attacks.

4. Analysing the existing prevention mechanisms and based on the study of existing techniques finding the solution to mitigate DoS attacks.

1.6 Contributions

The work presented in the dissertation presents a thorough study of *Availability* from the security perspective and analyses its importance in the present security paradigm. The main adversary of *Availability* i.e. DoS attack, its impact on *Availability*, and its modes of operation, existing countermeasures and the mitigation strategy are analysed and discussed keeping in view the current information infrastructure in the world of Information and Communications Technology. The major contributions of the thesis are as follows:

1. The thesis thoroughly discusses and analyses the role and importance of *Availability* in the current information security paradigm and provides an in-depth coverage of its association with other security attributes. While doing so a realistic shape of the existing CIA triad is given. Also during the study certain factors were identified that basically define, determine and measure Availability. Factors identified were:

a) At System level: Availability is dependent upon and determined by Reliability, Accessibility and Timeliness.

b) At component level: the design in the interacting components (software) can prove very critical in case of an adversarial and hostile environment. For the purpose a metric is derived and evaluated for an information system with CBD architecture.

2. The thesis discusses the system level determinants of *Availability* i.e. *Reliability, Accessibility* and *Timeliness* and provides an outlook of various metrics present in both theory and practice that determine or measure these attributes. An empirical evaluation of the question "how these attributes are affected by DoS attacks? And the effect in-turn resulting in impacting the *Availability* of an *Information System*" is also provided in the thesis.
3. The security discussion w.r.t to *Availability* goes beyond the system level in the thesis i.e. a quantitative metric based on the design of the interacting components (software) for evaluating *Availability* of an *Information System* is also given. The derivation, the algorithm and the evaluation of the algorithm is also done in the thesis. Algorithms for standalone systems and remote-based-component-composition systems is given in the thesis.
4. The thesis gives a comprehensive and a well-structured description on the problem of DoS attacks in internet. The thesis further elaborates how single source and distributed source DoS attacks are orchestrated. An analysis of most frequently occurring attacks in the recent times is also provided in the thesis.
5. The thesis provides as in-depth understanding of TCP-SYN DoS attack in the Internet. A detailed discussion on how the TCP protocol is exploited for executing a DoS attack. All the existing prevention methods regarding the TCP-SYN DoS attack are discussed and analysed in the thesis. Based on the study of the existing Hop Count Filtering technique we propose a *Victim Based Statistical Filtering (VBSF)* technique for the prevention of TCP-SYN type of DoS attacks. An algorithm and evaluation of the same is also given in the thesis.

1.7 Thesis Roadmap

The roadmap of the thesis is structured as follows:

Chapter 2 discusses **Availability.** The chapter starts with a discussion on the stance of Availability in the current information security paradigm and an in-depth analysis of the importance of availability in the CIA triad is also given. After this a detailed understanding of availability as a security attribute is given and the factors that can affect availability are also discussed in detail. A discussion on availability categories with respect to information system categorization i.e. *Basic availability, high*

availability and *continuous availability,* follows next. What follows next is an analysis of relation with other security attributes. The chapter ends with a discussion on availability and the possible adversaries that exist today and a conclusion on how availability should be treated in today's information security paradigm.

Chapter 3 discusses the **System level Determinants of Availability and the Impact of DoS Attacks**. The chapter starts with a discussion on the system level metric and determinants of Availability i.e. *Reliability, Accessibility* and *Timeliness* and provides a review of various metrics that determine or measure these attributes. The chapter provides an empirical evaluation of the effect of DoS attacks on these determinants by examining the certain parameters of metrics against DoS attacks. A detailed result analysis and a conclusion is also provided at the end of the chapter.

Chapter 4 discusses **the Design and Evaluation of Availability Metric at the Component level.** The chapter starts with a discussion on the need for such a metric, followed by a review of the attributes of dependability and security. A quantitative metric based on the design of the interacting components (software) for evaluating Availability of an Information System is proposed in this chapter. The derivation, the algorithm and evaluation are covered in the chapter.

Chapter 5 discusses **Denial-of-Service Attacks** in detail. The chapter starts with an in-depth analysis of single source DoS attacks and distributed-source DoS attacks (DDoS). It is followed by a detailed study of how these attacks are orchestrated in the Internet and for the purpose certain attack structures are presented. An analysis of the most frequently observed attacks in the recent years is also given in the chapter.

Chapter 6 discusses in detail the **Attack Structure of TCP-SYN Flooding** and the proposed **Prevention Framework.** The chapter starts with an in-depth discussion on how the TCP protocol is exploited for executing the TCP-SYN Flooding DoS attack. Certain well known prevention methods are analysed in the chapter. Based on the study of an existing *Hop Count Filtering* technique we propose a *Victim Based Statistical Filtering (VBSF)* framework for the prevention of TCP-SYN type of DoS attacks. For the purpose we present the *VBSF Algorithm* and then lastly the framework evaluation.

Chapter 7 discusses the conclusion and the future scope of the work. Immediately after the chapter follows the list of published work from the thesis.