CHAPTER 2

LITERATURE REVIEW OF NETWORK SECURITY

2. INTRODUCTION

We are in the information age; the number of people using computers and the internet are growing at a staggering rate day by day. The exponential growth in the internet users over the last decade has raised a number of concerns regarding network attacks for unauthorized access, denial of service, and confidentiality of the data. Thus, network security of personal computers, organizations, and government institutions became a major concern for protection of critical information from numerous network attacks. The exponential raise in internet users also made networks more complex and even more difficult to protect from network threats. The integrated network infrastructure comprising different data types like audio, video and textual information has introduced new loopholes in the network resulting in new types of attacks which takes network security concerns to next level of importance. Therefore, introducing latest technologies in the network infrastructure is becoming exceedingly challenging job for network managers. Hence there is a need to give critical importance to the security of the network.

To the core of this problem is the structure of the internet itself. Modifying the architecture of the network can reduce the possibility of attacks. The approach for security measures can be decided by knowing the method used for the network attacks. There are known approaches followed by many institutions to safeguard themselves from network attacks. The approaches like implementing firewall in the network, encryption and implementing intrusion detection systems IDS. One more approach is to create an “intranet” for being connected with internet yet maintaining security from possible network threats. The most important element in the information security is the network security system, which is securing all the information packets being exchanged within the computer connected to the network. Network security system provides an acceptable level of protection to the computer connected to the network by means of hardware, software, procedures, access controls and administrative regulations. One of the important functions of network security is to prevent data loss which follows basic elements as illustrated in Figure 2.1. The first element is integrity, which means the information stored in a secured network is accurate, unaltered and secured from data
corruptions. The second element is confidentiality, wherein the information shared on the internet (network) should be accessible to (intended) authorized users only. And the third element of a secured network is availability, which deals with making required information available to the authorized users at desired times without failure.

![Figure 2.1 Illustrates Basic principles of network security](image)

**2.1 HISTORY AND EVOLUTION OF NETWORK SECURITY**

In 1960s, the networks were in the form of isolated groups, connecting mainframes and multiple network nodes. Yet security of information across the network was the major concern although without client/server networks, time sharing, multiple users and multitasking processors. This problem gave rise to evolution of network security systems during the decade of 60s.

In 1969, the Defense Advanced Research Projects Agency DARPA has requested an institution with four computers to develop a network for exchange of information between two nodes the network. There are a number of institutions responsible for the birth of internet namely UCLA, the University of Utah, University of California at Santa Barbara and the SRI. The network invented was termed as ARPAnet, which started to grow with joining of the number of other organizations like academic institutions, defense related companies, and government organizations. The true need of the network
security emerged as the Transmission Control Protocol TCP and Internet Protocol IP were invented and became part of routine internet usage. The invention like the personal computer in 1980s, Local Area Network LAN and NSFNET laid the foundation for massive network security threats. The first Personal Computer PC is released by Apple computer in the early 1980s, followed by IBM releasing their personal computer. The discovery of hardware cards enabled IBM PCs to connect to mainframe computers. A company called Novell designed the first Local Area Network LAN which made network between PCs possible. In late 1980s, there was ever increasing number of PC and LAN users.

Simultaneously, The National Science Foundation NSF, an agency of the U.S. government developed a NFSNET having five super computer centers in a network. Thus, these developments made internet available to everyone who had the required hardware and software to connect to the network. This is adding to existing concerns regarding network security issues due to increased amount of information is being exchanged between many nodes on the Local Area Networks and internet. The government developed a Trusted Computer Security Evaluation Criteria, in which these serious security issues were addressed by developing security guidelines.

In 1988, the first internet virus was launched, and the importance of an effective network security system was witnessed by the entire world as all 60000 computers in the network were affected by the virus attack. In the recent past, more than two million computer users joined internet. In this way the security of the network gained top line of concern for the first time since the invention of PC. Since this massive infrastructure of the internet has not developed any means for protection of itself from attacks. The exponential growth in the internet users raised critical issues related to security as the size, complexity and dependency on the network causes further complications.

In recent years the intrusion techniques have evolved from simple methods like tracing passwords, exploiting vulnerabilities and social engineering attacks to more advanced methods like exploiting protocols flaws, defacing web servers, installing sniffer programs, denial of service attacks, distributed attacks and developing command and control networks to used compromised computer to launch attacks, Figure2.2 shows entire vulnerabilities reported (1995-2003):12,946[CC06a].
The numbers of security incidents increased dramatically due to the sudden increase in vulnerabilities and intrusion profiles in recent years. These values indicate a very alarming condition wherein there is an increase in expertise of an intruder. The complexity of network and system administration is also increasing. On the other hand the ability to react quickly is decreasing significantly and on top of which vendors continue to produce software products with inherent vulnerabilities. Many approaches tried to provide security at the host or network; the approaches include antivirus, spyware, firewall and authentication systems. These approaches however provided security up to some extent but still faced many challenges due to system flaws, operating system bugs and social engineering attacks.

The concept of intrusion detection system IDS was proposed by James Anderson in 1980. Followed by three IDS models based on detection intrusion, Anomaly detection, Misuse Detection and Hybrid Detection proposed in 1988. The normal user operations are defined in anomaly detection based IDS, and any changes in the normal operation are identified. But in this type high rate of false positive is observed which can be problematic. The detection of intrusion is achieved by observing pattern of traffic or application data in misuse detection based IDS. This type of intrusion detection produces less number of false positive since it compares observed patterns with predefined signatures. In this case the database of signatures needs to be updated to maintain an acceptable level of protection.

The anomaly based detection approach is combined with misuse based detection approach is termed as hybrid detection based IDS.

There are three types of IDS: Host based IDS, Network based IDS and Hybrid based IDS. Analysis of system status, processes running and integrity of files on the particular system on which the IDS is installed is done by host based IDS. Whereas every packet transmitted over the network is analyzed by network based IDS. Hybrid based IDS combines’ advantages of both. An IDS processes the information by either centralized or distributed way. The information is gathered and sent to one point in a network in centralized method wherein in the distributed method the information can be processed at various locations in the network. The advantage if distributed information processing is that it has better scalability, but still it is insecure from the network attacks.
Since most of the current IDS depend on system administrator they failed to detect and respond to intrusion in real-time. To be able to respond in real time the administrator needs to analyze enormous logs generated by traffic on the network, identify the attack and respond to it which is significantly difficult. This problem is exploited in zero day attacks; as it leaves a way open to attackers because of the time delay in the identification and response by administrator.

Software applications also has inherent security vulnerabilities, normally such vulnerabilities are not identified in real time due to large size of networks and lack of access to knowledge of latest vulnerabilities in software by administrator. The care should be taken in installing latest released patch at required places as soon as possible. The scarcity of automated security management tools also acts as a catalyst which helps in intrusion attacks. Not implementing proper security management tasks like enabling firewall, IDS and scanning leaves system vulnerable to attacks although vulnerabilities in software are discovered and patched.

Figure 2.3 shows the vulnerability exploit life cycle. Vulnerability should be detected and patched prior to crude exploit tool used at level 3[CC06b].
The Figure 2.4 from US-CERT shows how the cyber incidents rose in the current internet network environment; this gives requirement of IDS deployment in network security model.
2.2 NETWORK SECURITY ATTACKS

Network security is of critical importance for all sorts of organization. An intruder can be very harmful if the network security is broken. An awareness and education needs to be spread to the computer users regarding securing their systems from network attacks. Being up to date with the newly released patches and fixes is very crucial, without which it becomes easy for a hacker to gain unauthorized access to the user’s information. There are different types of attacks on a computer system or network security depending upon viewing the function of computer as providing information. Generally the information flows from source to destination i.e. from source file or user to the destination file or user. In general, there is a flow of information from a source, such as a file or a region of main memory, to a destination, such as another file or a user. Some basic network security attacks are described below [KD07] [CKC10]:

1. **Eavesdropping Attacks**: in this type of attacks the network communication is intercepted in an unauthorized manner in such a way that the network information is disclosed to the attacker. This type of attack can be performed at the network layer by sniffing into the information packets or at the physical layer by tapping the medium for accessing information (cabling or wireless medium).

2. **Logon Abuse Attacks**: this type of attack enables a user to obtain access with additional privileges than he is authorized to have. Such attacks would overcome the authentication and access control mechanisms.

3. **Spoofing Attacks**: in this type of attack the subject puts forward an identity which that the subject has no right to use. This can be illustrated by using an example of IP spoofing attack. In an IP spoofing attack the System is convinced by an attacker that it is exchanging information with known principals resulting in providing access for critical information to the attacker. This is achieved by sending a packet with an IP source address of known and trusted host by changing the packet at the transport layer. Therefore, the destination host may be deceived and accepts the changed packet as valid packet.

4. **Intrusion Attacks**: This is one of the most dangerous type of attack in which an unauthorized user that is attacker gaining access to the system through the network. Generally this type of attack would exploit specific vulnerabilities present. For an
example, a web server intrusion attack is a buffer overflow attack, wherein a web service acts in an unpredictable manner because it receives more data than it is intended to receive.

5. Hijacking Attacks: under this type, an attacker tries to obtain unauthorized access to the system. These attacks are essentially attempts to gain unauthorized access to a system by using an authorized entity’s existing connection. For example, if an authorized user of the system leaves a session open, not closing it properly then such a situation can be subject to session hijacking by an attacker.

6. Denial-of-Service DoS Attacks: these type attacks utilizes the network or server resources to make it unavailable (not in usable condition) for the authorized user. The advance type of such attacks is the distributed denial-of-service DDoS attacks, wherein the resources from the distributed environment are used by the attacker against target host. For example, SYN attack and Ping of Death attack.

7. Application-Level Attacks: the flaws in the security measures of application layer are exploited in this type of attack, wherein in most of the cases, intrusion is the main motive of the attacker. For example, a web server having security issues with the technology adopted while implementing web site or faulty controls in the filtering of an input on server. This type of attacks is best demonstrated by examples enlisted below: malicious software attacks (Trojans, viruses), Web server attacks, Structured Query Language SQL injection, remote command execution and cross-site scripting (XSS). Further security attacks are divided into two types:

2.2.1 Passive attacks
In this type of attack, the information transmitted or received by an authorized user is detected and monitored by the attacker without the notion of the user of the network. Passive attacks generally breaks confidentiality measures but leaves original information unaltered since the motive of the attacker is to gather information. Passive attacks are also differentiates through the fact that they violate the confidentiality rules and do not produce damages, do not delete or modify the data. The target of the opponent is to get information that is being transmitted. A passive attack is generally harder to detect as
there is small effect to the information communicated. Two kinds of passive attacks are [sta11] [BD08]:

1. **Release of message content**: is simply realized, a telephone talk, an electronic mail message, and a conveyed file can include sensitive or confidential information.

2. **Traffic analysis**: is a kind of passive attack where a hacker examines the patterns in communication on a network. It is referred with only masking the contents of conveyed files and is extra delicate than other types of attacks sequentially that opponents, even though they captured the message, but they could not extract the information from the message. The general technique for masking contents is encryption.

   If we had encryption protection in position, an opponent might be able to monitor the pattern of these messages. The opponent could decide the location and identity of communicating hosts and might monitor the frequency and length of messages being exchanged. This information might be helpful in guessing the nature of communication that was going on [Sta11] [BD08].

2.2.2 **Active attacks**

These attacks plan several modification of the data stream or the making of a false stream, and cannot be prevented easily dissimilar a passive attack. These attacks can be subdivided into four types [BD08] [Pat09] [Sta11]:

1. **Masquerade**: a masquerade is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for. Such as, confirmation sequences can be captured and replayed subsequent to an applicable authentication series has taken place, thus enabling a sanctioned entity with some privileges to get extra privileges by impersonating an entity that has those privileges.

2. **Replay**: it is the intention the passive capture of a data unit and its following retransmission to generate an unauthorized result. A replay attack is a type of network attack in which an applicable data transmission is maliciously or fraudulently repeated or delayed. This is passed out either by the creator or by an opponent who intercepts the data and retransmits it.
3. **Modification of the message:** It purely means that some bit of a genuine message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.

4. **Denial of service:** is produced by the accidental failure of nodes or malicious action. This attack is an enveloping threat to nearly all networks. It stops or inhibits the usual use or management of communications facilities. Sensor networks being extremely energy-sensitive and resource-limitation, they are very vulnerable to DoS attacks. This attack may have a particular target. Such as, an entity may suppress all messages aimed at a specific destination (e.g., The security audit service). One more type of service denial is the disruption of a whole network, either by disabling the network or by overloading it with messages so as to humiliate performance.

### 2.3 SECURITY SERVICES

Security services improve security of data processing systems and information transfers of an association and meant to contradict security attacks. Security services offer confidentiality, integrity, and availability services for the platform. Security services are implemented as protection services, such as authentication and authorization, detection services, such as supervising and auditing and response services, such as event response and forensics. There are six key categories of security service [BD08] [Pat09]:

1. **Authentication:** this service can be used to establish that the claimed uniqueness of a communicating principal is valid (peer entity authentication) or that the maintained source of a data unit is valid (data origin authentication).

2. **Access Control:** this mention to the capability to control the level of admittance that individuals or entities have to a network or system and how much information they can get. This service may be useful to several types of access, such as read, write, or execute or combinations of the above. Access to resources might be controlled through a variety of types of access policies, similar as rule-based or identity-based security policies. The access control services should assist with the authentication services, seeing as permitting access rights to a principal requires former authentication of the principal requesting a specific access.

3. **Data confidentiality:** this mentions to the security of information from illegal disclosure. Confidentiality is categorized into connection confidentiality (when it engages
the entire layers of the communication), connectionless confidentiality (when it offers confidentiality in a connectionless service data unit), choosy field confidentiality (when it guards choosy fields of the data), and traffic flow confidentiality (when it protects information that could be potentially obtained from inspection of traffic flows).

4. **Data integrity:** this refers to the capability to guard information, data, or transmissions from illegal, unrestrained, or accidental alterations. The term integrity can also be used in reference to the functioning of a network, system, or application. This service might have a number of forms. Connection integrity with recovery provides integrity of the data and also detects modification, insertion, deletion, and replay of data. Selective field connection integrity provides integrity for selective data fields within a connection.

5. **Non-repudiation:** this mentions guarantees that a principal cannot reject the transmission or the receipt of a message. This service might take one or both of two forms. With non-repudiation with evidence of origin the recipient of data is provided with evidence of the origin of data, so that the dispatcher cannot afterward deny that he/she sent the specific data. With non-repudiation with evidence of delivery the dispatcher of data is provided with evidence of the delivery of data, so that the receiver cannot afterward deny having received the specific data.

6. **Availability:** a diversity of attacks able to result in the loss of or reduction in accessibility. This mentions to whether the network, system, hardware, and software are dependable and may recover speedily and completely in the event of an interruption in service. Ideally, these components should not be prone to denial of service attacks.

2.4 **Security Mechanisms**

Security mechanisms are methods to detect, prevent, or recover from a security attack. It is important for systems to have implemented as many security mechanisms as potential equally essential for their system. Security mechanisms can be divided into two categories [BD08][KD07]:

2.4.1 **Specific security mechanisms**

The implementation of the security services is offered through specific security mechanisms. These may also be separated into some types:
1. **Encipherment mechanisms:** these mechanisms supply data confidentiality services by converting the data to forms which are not readable by unauthorized principals. And the use of encryption or cipher algorithms, also the source of some authentication exchange mechanisms.

2. **Digital signature mechanisms:** digital signatures are the electronic equal as of ordinary signatures in electronic data. These types of mechanisms are built by accurately applying asymmetric encipherment. It consists of two procedures, signing procedure which is private and verification procedure which is public. It can offer non-repudiation, origin authentication and data integrity services and similarly on the basis of some authentication exchange mechanisms.

3. **Access control mechanisms:** the access control mechanisms are used to supply access control services. These mechanisms can make use of the authenticated identity of an entity or other information associated with an entity (e.g. Membership, permissions, or capabilities of the entity) in order to decide and impose the access rights of the entity. The access control mechanisms can also report unauthorized access attempts as part of a security audit trail.

4. **Data integrity mechanisms:** deliver protection against modification of data, and used to supply data integrity and origin authentication services, also on the basis of some authentication exchange mechanisms. Two categories of data integrity, one which concerned with integrity of single data unit and other are concerned with a complete data sequence.

5. **Traffic padding mechanisms:** these mechanisms supply protection from traffic analysis attacks. Some network protocols and security mechanisms contains padding mechanisms to guard the exchanged communication. These can be operative only if the traffic padding is protected by a confidentiality service.

6. **Routing Control Mechanisms:** these mechanisms permit the collection of a specific route for the communicating data either dynamically or statically through prearranged ways. Furthermore, by applying security policies, data carrying certain security labels may be routed through certain sub networks, relays, or links. Hackers, viruses, and malicious programs often exploit the security vulnerabilities of routing protocols in order to introduce network security attacks.
7. **Notarization mechanisms:** At the time of sending or delivering of transmitted data notarization mechanisms are used to assure the integrity, the source or destination. These assurance mechanisms may be an amount of the networking protocols in use and/or of a trusted third party which may be used to assure the communication reliability and non-repudiation. A notarization mechanism may be maintained by other mechanisms such as digital signatures, encipherment, or integrity mechanisms.

**2.4.2 Pervasive security mechanisms**

The implementation of the security services is supplied over pervasive security mechanisms. This mechanism is not definite to particular services. These can also be separated into numerous sets [BD08]:

1. **Trusted functionality:** it can be used either to extend the range or to establish the efficiency of other security mechanisms. Whichever functionality that directly provides security mechanisms, or provides access to those, should be responsible.

2. **Event detection:** exposure of security related events.

3. **Security label:** the marking assurance to the resource is that names or describes the security attributes of that resource. Frequently necessary to transfer the appropriate security label with data in transfer. A security label may be supplementary data connected with the data transferred or may be implicit.

4. **Security audit:** it mentions to an autonomous analysis and examination of system records and activities in order to test for capability of system controls, to guarantee compliance with recognized policy and operational procedures, to identify breaches in security, and to mention any specified changes in control, policy, and procedures.

5. **Security recovery:** it transactions with needs from mechanisms, such as event handling and management functions, and takings recovery actions.

**2.5 MALICIOUS SOFTWARE**

Malicious software (malware) permits an intruder to capture or damage a target host without the owner’s permission and frequently without his or her knowledge. More than the past thirty years, malware has grown to be a more dangerous worldwide problem as Internet-connected computers contain proliferated and operating systems have become
more complex. Nowadays, the average PC user must be extra aware of computer security than ever before as a result of the constant threat of possible infection. Even though accurate costs are hard to determine, there is small doubt that malware has widespread effect on equipment damages, loss of data, and loss of productivity. According to surveys, malware is one of the most ordinary and costly types of attack on organizations [CT]. In the beginning of computing, malware was mostly viruses and Trojan horses that spread among computers generally by floppy disks and shared files. In the present day, malware is mainly worms, viruses, spyware, bots, and Trojans proliferating through computer networks. Worms are a specific concern due to their ability to increase by themselves during computer networks. They can exploit weaknesses in operating systems or general applications for example Web and email clients. They are regularly used as vehicles to install other types of malware onto hosts. Several thousands of worms and viruses are regularly tracked by the WildList [WOI06] and antivirus companies.

Logically, host-based and network-based defenses have also evolved in the superiority in response to rising threats. Surveys have found that organizations almost universally use antivirus software, firewalls, intrusion detection systems, and additional means of protection [GLM+06]. These defenses definitely block a tremendous amount of malware and avoid global disasters. On the other hand, their usefulness is widely known to be restricted by their ability to accurately detect malware. Detection accuracy is critical because malware has to be blocked without interfering with legitimate computer activities or network traffic. This complexity is compounded by the creativity of attackers constantly attempting to create new methods to avoid detection [SB08] [Sta11].

### 2.5.1 Types of Malware

There are different types of malware are generally depicted as viruses, worms, Trojan horses, backdoors, root kits or spyware. These terms correspond to the functionality and performance of the malware (e.g. a virus is self-broadcasting, a worm is self-replicating). Several major types of malware are described below [Mal08] [Mal09], Figure 2.5 malware and phishing sites monitored by AusCERT.

- **Backdoors**: a backdoor is malicious code that permits illegal right of entry to a computer system or network by accepting remote commands from an attacker somewhere
else on the Internet. Backdoors permit attackers to execute remote commands and install other software, which may in turn compromise passwords or other personal data, or permit the machine to be used for additional nefarious reasons [Nis].

- **Keystroke loggers**: a keystroke logger is an unseen program that records and “logs” each key that pressed on the compromised system keyboard, as the valid user of the system is typing, in the process recording personal data similar to usernames, passwords, credit card and bank account numbers. Keystroke loggers secretly accumulate the data away in hidden files that are ultimately transmitted to a remote collection point, away across the network.

- **Root kit**: a root kit is a set of programs designed to cover up the negotiation of a computer at the most advantaged “root” level, by modifying operating system files or inserting code into the memory of running processes. As with most malware, root kits needed administrative rights to run efficiently, and once installed can be practically impossible to detect [AC07].

- **Spam**: spam is normally understood meaning bulk, unsolicited, unwanted and potentially harmful electronic messages [OEC07].

- **Spyware**: spyware is a type of malware that is capable of capturing a range of data from user input (keyboards, mice) and output (screens) and other storage (memory, hard drive etc.) And transferring this information to the attacker without the user’s permission or knowledge.

- **Trojan horses**: a Trojan horse is a computer program that comes out legitimate but actually has unseen functionality used to circumvent security measures and perform attacks. A Trojan horse may enter a user’s computer by presenting itself as a compellingly attractive tool of some sort which the user purposely downloads and installs, unaware of its hidden reason. Trojans typically make in the functionality of key loggers and other spyware and a range of other functions to disable system security.

- **Virus**: a virus is unseen code that spreads by infecting an additional program and inserting a copy of itself into that program. A virus requires its host program to run before the virus can become active and usually requires human interaction to activate.

- **Worm**: a worm is a type of malware that self-repeats without the need for a host program or human interaction. Worms usually exploit limitations in a computer operating
system or other installed software and spread speedily from computer to computer across a network and/or the Internet.

- **Logic bomb**: a program inserted into software by an intruder. A logic bomb lies dormant until a predefined condition is met; the program then generates an unauthorized act [Sta11].
- **Mobile code**: software (e.g., script, macro, or other portable instruction) that can be crafted unchanged to a heterogeneous collection of platforms and carry out with identical semantics [JW01].
- **Auto-rooter**: malicious hacker tools used to break into new machines remotely.
- **Flooders**: used to attack networked computer system with a huge volume of traffic to execute a denial-of-service (DoS attack) [Sta11].
- **Zombie, bot**: program activated on an infected machine that is activated to a launch attacks on the other machine [Sta11].

![Figure2.5](Malware and phishing sites monitored by AusCERT\(^1\))

\(^1\)AusCERT constituents are its members and Australian Internet users in the public and private sector, home and business. For more details, see references: APCERT Annual Report 2010, http://www.apcert.org
2.6 DISTRIBUTED DENIAL OF SERVICES (DDoS) ATTACKS

In early year 2001, a new category of DoS attack became pervasive, called a Distributed Denial of Service attack, or DDoS. In this type, several comprised systems are used to attack a single target. The overflow of incoming traffic to the target will frequently force it to shut down. Distributed Denial of Service (DDoS) attacks have become more cultured in the previous several years as the level of attack computerization has amplified. Distributed Denial of Service (DDoS) attacks are becoming a progressively consistent disturbance of the worldwide Internet. They are very hard to protect against because these attacks consume resources at the network and transport layers, where it is hard to validate whether an access is genuine or malicious. There are two purposes for DDoS attacks, the first is to consume the resources of the host and second is to consume the bandwidth of the network. Contemporary schemes are to defend the resources of the host drop incoming packets according to fields, for example protocol type and port number. Though, the drawback in doing this are that there is no precise way to distinguish the usual traffic from the malicious traffic. The usual traffic could be disturbed by comprehensively dropping packets. DDoS attack is attractive much the same as a DoS, but the dissimilarity in results is huge; as its name suggests the DDoS attack is implemented using a circulated computing method frequently mentioned to as a 'botnet army', the making process of which contains infecting computers with a form of malware that provides the botnet owner access to the computer slightly this could be whatever from basically using the computers connection to flood to whole control of the computer. These attacks affect the victim’s computer server more than a consistent DoS because many connections are being used against one connection [MD08] [MAS11]. A DDoS attack can be depicted as follows Figure 2.6.
Recruitment: The attacker selects the vulnerable agents, which will be used to perform the attack.

Compromise: The attacker exploits the vulnerabilities of the agents and plants the attack code, guarding it concurrently from discovery and deactivation.

Communication: The agents inform the attacker through handlers that they are ready.

2.6.1 DDoS Defense Mechanisms

There are lots of DDoS defense mechanisms. We introduce them using two standards [DM06] [DS07]:

2.6.1.1 The activity deployed by the attacked

DDoS defense mechanisms according to the activity arranged can be divided into the following four types:

1. Intrusion Prevention: The best improvement strategy against any attack is to completely prevent the attack. In this phase, we try to stop DDoS attacks from being launched in the first place. There are several DDoS defense mechanisms that attempt to prevent systems from attacks:
• **Using globally coordinated filters:** [FS01] [San] [PL01] [PLR03] attacking packets can be blocked before they cause serious damage. There are lots of filtering mechanisms that can be used, together with ingress filtering, egress filtering, route-based distributed packet filtering, history-based IP (HIP) filtering, and secure overlay services (SOSs).

• **Disabling unused services:** is another way to avoid DDoS attacks. If network services are not required or idle, the services should be disabled to prevent attacks. For example, if UDP echo is not essential, disabling this service will build the system extra secure against this kind of attack [GW00].

• **Applying security patches:** can shield the hosts against DDoS attacks. Every computer host should update according to the most recent security patches and use all the existing security mechanisms to combat DDoS attacks [GW00].

• **Changing the IP address:** is an easy way to secure against a DDoS attack. This technique is identified as “moving the target defense.” All Internet and edge routers are informed when the IP address is changed in order to drop malicious packets. This option can be used only for local DDoS attacks based on IP addresses. Though, attackers can provide this technique of useless by adding a DNS tracing function to the DDoS tool [GW00].

• **Disabling:** IP broadcasts; we able to prevent the use of host computers as reflectors in Smurf and ICMP flood attacks. We should make clear that this intrusion prevention mechanism can be successful only if all the neighboring networks have also disabled IP broadcasts [LRS+00].

• **Load balancing:** is a simple way that enables network providers to raise the supplied bandwidth on critical connections and prevent their crash in case an attack is launched against them. Supplementary reliable protection can be the replication of servers in case several crash during a DDoS attack [SL03].

• **Honey pots:** can be used to prevent DDoS attacks. Honey pots are not extremely secure systems and can be used to ruse the attacker to attack the honey pot instead of the system being protected. Honey pots possibly used not only for the protection of systems but also to get some additional information about the actions of the attackers. Honey pots are based on the design of luring the attacker into thinking that he/she has successfully compromised the system (e.g., Honey pot), causing the attacker to install either the
handler or the agent code that is in the honey pot. Therefore, systems can be protected from possible DDoS attacks [Wei02][Mir00].

2. **Intrusion Detection:** Intrusion detection can be used to protect a host computer or network against existing a source or a victim of an attack. Intrusion detection systems detect DDoS attacks either by using a priori knowledge of the kinds of known attacks (signatures) or by identifying deviations from ordinary system behaviors.

- **Anomaly detection:** trusts on identifying behaviors that are irregular with respect to several regular standards. Various anomaly detection systems and approaches have been established to identify the weak signs of DDoS attacks.

- **Misuse detection:** uses a priori knowledge on intrusions and tries to notice attacks created on specific patterns or signatures of known attacks. These patterns are defined as intrusion signatures. Even though misuse detection systems are exact accurate in detecting known attacks, their basic disadvantage is that attacks are under continuous development, and this leads to the essential for an update knowledge base of attacks. Numerous popular network monitors accomplish signature-based detection, for example CISCO’s NetRanger, Secure Net, Bro, Real Secure, NFRNID, and Snort.

3. **Intrusion Response:** once an attack is recognized, the after that step is to recognize the source and obstruct its traffic consequently. The obstructing part is typically performed under manual control (e.g., by contacting the administrators of upstream routers and enabling access control lists) since an automated response system might cause additional service deterioration in reply to a false alarm. Automated intrusion response systems are installed only after a period of person learning (for the ones that employ neural computation in order to discover the DDoS traffic) or testing (for the ones that operate on static rules). There are a lot of ways that goals the tracing and recognizing of the actual attack source.

- **IP trackback:** traces the attacks back to their source; thus one can discover the right individuality of the attacker and accomplish detection of asymmetric routes as well as path characterization. Few aspects that render IP trace back hard is the stateless nature of Internet routing and short of source responsibility in TCP/IP. For competent IP trace back, it is required to compute and construct the attack path. At an extremely fundamental level, IP trace back can be thought of as a process that is performed
manually in which the administrator of the network that is the sufferer of an attack calls the ISP in order to be educated of the direction from which the packets are originating. Cause of the complexity of the manual trace back, there have been a lot of proposals that attempt to make this process easier and automatic, for example, ICMP trace back [Bel00], link-testing trace back [BC00], probabilistic packet marking (PPM) [SWK+01], hash-based IP trace back [SPS01], Sleepy Trace back [WRW01], and Center Track [Sto00].

- **Traffic pattern analysis:** is one more approach to react to DDoS attacks. During a DDoS attack, traffic pattern data can be stored and then analyzed subsequently the attack in order to discover specific characteristics and features that can point out an attack. The results from this analysis of data may be used to update load balancing and limiting techniques as well as produce fresh filtering mechanisms that stop DDoS attacks [SL03].

- **Analysis of event logs:** is one finer approach that goal the response to DDoS attacks. The choice of event logs recorded during the setup and the execution of the attack may be used to find out the type of DDoS attacks and do a forensic analysis [SL03]. Network equipment similar as firewalls, packet sniffers, server logs, and honeypots can be used in the choice of event logs [Wei02].

### 4. Intrusion Tolerance and Mitigation:

Investigation on intrusion tolerance accepts that it is unfeasible to avoid or stop DDoS attacks totally and spotlight on reducing the attack affect and increasing the excellence of its services. Intrusion tolerance can be divided into two categories: fault tolerance and quality of service (QoS).

- **Fault tolerance:** is a research region whose designs are created in critical infrastructures and utilized in three levels: hardware, software, and system [Nis95]. The proposal of fault tolerance is that by copping the network’s services and employing diverse access points, the network can go on offering its services when flooding traffic congests one network link.

- **Quality of service QoS:** illustrates the capability of a network to distribute expected results for few applications. A lot of intrusion-tolerant QoS techniques and intrusion-tolerant QoS systems have been developed to moderate DDoS attacks. In the midst of intrusion-tolerant QoS techniques integrated (IntServ) and differentiated services (DiffServ) stand for the principle architectures [ZOS00]. Queuing techniques are also employed to fight DDoS attacks. The matured and mainly broadly applied queuing
technique is class based queuing (CBQ). CBQ sets up diverse traffic queues for dissimilar types of packets [KMW01]. A total of outbound bandwidth can then be assigned to each queue. Additional intrusion-tolerant QoS systems are VIPnets, proactive server roaming, resource accounting, resource pricing, pushback, and throttling [Bru02].

2.6.1.2 The location deployment of the attack
DDoS protection mechanisms are divided in to those deployed at the victim, intermediate, and source network based on the deployment site.

1. **Victim-Network Mechanisms:** large amount systems deployed to protect against DDoS attacks have been designed to work on the victim’s network, since this will experience the mainly from an attack. The victim is the one that wants to be defended against a DDoS attack so it is the one that should deploy a DDoS defense system [Mir00]. Similar kind of system will boost a victim’s a capacity to identify that it is the objective of an attack as well as to gain more time to respond. Note, though, that to accomplish increased security the victim’s network will forfeit few of its performance and resources.

2. **Intermediate-Network Mechanisms:** DDoS protection mechanisms installed at the intermediate network which are further efficient than victim network mechanisms since the attack traffic can be handled simply and find the origin of the attack. An example is WATCHERS [BCP+98]. Though, these protection mechanisms present a number of limitations that stop their broad deployment, such as the amplifying of the intermediate network’s performance and the superior complexity to identify the attack since the intermediate network usually is not affected.

3. **Source Network Mechanisms:** DDoS protection mechanisms installed data the source network can discontinue attack flows ahead of they enter the internet core. This means that it is simple to protect against them before the total with one more attack flows. Furthermore, being lock to the source creates it simpler to trace back to the source of the attack. A source network mechanism has the same limitations as the transitional network mechanism of detecting the incidence on an attack, since it does not knowledge any difficulties. This disadvantage can be balanced by its capability to give up few of its resources and performance in order to accomplish better DDoS detection. On the other
hand, the main limitation of such a system is that in the case of unreliable attack detection legitimate traffic might be limited.

2.7 DENIAL OF SERVICES (DoS) ATTACKS
A DoS attack can be illustrated as an attack designed to make a computer or network incompetent of providing usual services. A DoS attack is considered to take place only when access to a computer or network resource is purposely blocked or deteriorated as a result of malicious action taken by another user. These attacks do not essentially injure data directly or everlastingly, but they purposely negotiation the accessibility of the resources. The mainly common DoS attacks target the computer network’s bandwidth or connectivity. In bandwidth attacks the network is flooded with a high volume of traffic leading to the exhaustion of all existing network resources, so that lawful requests cannot get through, resulting in deteriorated productivity. In connectivity attacks a computer is flooded with a high volume of connection appeals leading to the exhaustion of all available operating system resources, thus depicting the computer unable to process legitimate user requests [MD08].

2.7.1 Types of DoS Attacks
DoS attacks can be divided into five categories based on the attacked protocol level [KL01], as illustrated in Figure 2.7:

1. DoS attacks on the network device level contain attacks that may be caused either by receiving advantage of bugs or weaknesses in software or by exhausting the hardware resources of network devices. One example is caused by a buffer exceed error in the password inspecting routine. By means of this, certain routers could crash if the connection to the router is executed by way of telnet and very long passwords are entered.

2. At the operating system OS level DoS attacks take advantage of the ways protocols are implemented by OSs. One example in this type is the ping-of-death attack [KM97]. In this attack, Internet Control Message Protocol ICMP echo requirements having data sizes larger than the maximum Internet Protocol IP standard size are sent to the victim. This attack often has the effect of crashing the victim’s machine.
3. Application-based attacks try to settle a machine or a service out of order either by exploiting bugs in network applications which are running on the objective host or by using such applications to exhaustion the resources of their victim. It is also potential that the attacker may have created points of high algorithmic difficulty and exploits them in order to consume all obtainable resources on a remote host. One example of an application-based attack is the finger bomb [xforce]. A malicious user could origin the finger routine to be recursively implemented on the victim in order to exhaustion its resources.

4. In data flooding attacks, an attacker tries to use the bandwidth available to a network, host, or device at its highest range by transferring it to massive quantities of data to process. An example is flood pinging.

5. DoS attacks based on protocol features gross benefit of certain standard protocol features. For example, some attacks exploit the fact that IP source addresses can be spoofed. Furthermore, some categories of DoS attacks try to attack the domain name system DNS cache on name servers. An easy example of attacks exploiting DNS is when an attacker possessing a name server traps a victim name server into caching false records by enquiring the victim about the attacker’s own site. A vulnerable victim name server would then state to the malicious server and cache the answer [Dav99].

Figure 2.7 [Classification of remote DoS attacks]
2.7.2 DoS Defense Problems
In the subsequent, we present certain issues that create protection from DoS attacks is very difficult [XBZ01].

1. Highly Interdependent Internet Security
The Internet has a small number of built-in protection mechanisms to deal with DoS attacks. Its design releases security issues that can be exploited by attackers. It is essential to note that no matter how secure a host is it is constantly under risk while the rest of the Internet is unsafe.

2. Inherently Difficult to Detect DoS Attacks
Identifying the origin of DoS attacks is somewhat hard. Taking advantage of the stateless nature of the Internet, attackers take use of IP source address spoofing to hide the identity of the attacking machines and hide their identity behind handler machines. Moreover, DoS streams do not present some common features of DoS streams that we can use to detect DoS attacks. So the dissimilarity of attack packets from valid packets becomes enormously hard.

3. Limited Resources
The big numbers of packet streams that require to be produced in massive DoS attacks necessitate great amounts of resources. The systems and networks that contain the Internet are composed of limited incomes that can be effortlessly exhausted throughout the detection of DoS attacks.

DoS tools are accessible on the internet accompanied with commands that permit informal and effective use even from nontechnical skillful users. The attackers continuously effort to develop additional efficient tools in order to bypass security systems developed by system managers and researchers.

5. Target-Rich Environment
There are numerous hosts and networks in the Internet that are vulnerable and can be exploited and deliver productive ground to launch DoS attacks. Many Internet users do not have sufficient technical skills or are not security conscious and cannot guard their systems against DoS attacks. Furthermore, the design of an operative DoS system is a
problematic task that faces numerous challenges. The supplies for an effective answer to a DoS attack are the following [Mir03][Zar02]:

- One of the primary features of a DoS defense system is the extraordinary security. It must be safeguarded that a DoS defense system cannot be used as a victim of a DoS attack.
- A DoS defense system should be dependable in detecting DoS attacks and have no false positives. Though, because this can come at a high cost, we may not be very tough with this requirement.
- A DoS defense system should be competent in noticing and responding to a DoS attack in order to mitigate the effectiveness of the attack.
- A DoS defense mechanism should be genuine in design and applicable in existing security infrastructures without necessitating significant changes in the Internet infrastructure.
- A DoS defense mechanism should not necessitate several resources and should have short performance cost to avoid the deterioration of the performance of the attacked network.

2.8 A FIREWALLS

A Firewall is a part of software or hardware that filters all network traffic between a protected or “inside” network and a less dependable or “outside” network. Firewalls implement a security policy, which differentiate “good” traffic from “bad” traffic. Part of the challenge of protecting a network with a firewall is establishing the security policy that gathers the needs of the installation [Wen06]. A firewall system exclusive of an Internet access security policy cannot be properly configured. A policy exclusive of enforced procedures is worthless as it is unnoticed [Cha05] [Men10] Figure 2.8 illustrates a Firewall Structure.
2.8.1 Features of Firewalls

1. **Block incoming network traffic based on the source or destination:** jamming unwanted incoming traffic is the most ordinary feature of a firewall.

2. **Block outgoing network traffic based on source or destination:** a lot of firewalls may also screen network traffic from your internal network to the Internet.

3. **Block network traffic based on content:** further sophisticated firewalls may monitor network traffic for undesirable content. Such as, a firewall that is incorporated with a virus scanner may put off files that include viruses from incoming your network. Further firewalls integrate with e-mail services to screen out undesirable e-mail.

4. **Make internal resources available:** even though the main principle of a firewall is to stop unnecessary network traffic from passing through it, you may also configure lots of firewalls to permit selective access to internal resources, similar as a public Web server, whilst still stopping other access from the Internet to your internal network.

5. **Allow connections to the internal network:** a general process for employees to connect to a network is using virtual private networks (VPNs). VPNs permit protected connections from the Internet to a corporate network.
6. **Report on network traffic and firewall activities:** when screening network traffic to and from the Internet, it is also significant to be acquainted with what your firewall is doing, who tried to crack your network, and who tried to access improper material on the Internet. The majority firewalls consist of a reporting mechanism of few types or another.

2.8.2 **Firewall Design Principles**

As network traffic passes through the firewall, the firewall chooses which traffic to forward and which traffic not too forward, based on rules that you have defined. All firewalls monitor traffic that enters into your network, but a superior firewall ought to also monitor outgoing traffic. Usually a firewall is established where your internal network connects to the Internet. Even though bigger organizations can also put firewalls between dissimilar parts of their own network that need different levels of security, many firewalls monitor traffic passing between an internal network and the Internet. This internal network may be a particular computer or it may include thousands of computers. A network security domain is an adjacent area of a network that functions under a single, standard security policy. At any time domains intersect, there is a possible requirement for security to control traffic permitted into the network. Firewall technology can be used to sieve this traffic. The most general boundary where firewalls are applied is between an organization’s internal network and the internet [Woo04].

2.8.3 **Firewall Types**

There are four types of Firewall:

2.8.3.1 **Packet Filtering Firewalls**

The initial generation of firewall architectures emerged around 1985 and arrived out of Cisco's IOS software division, these are identified as a packet filter firewalls [IT04a]. Packet filtering is frequently performed by a router as part of a firewall. A usual router makes a decision where to direct the data, a packet filtering router chooses if it should forward the data at all. Packet filtering rules can be set on the following: physical network interface the packet arrives on, source or destination IP address and the type of transport layer TCP, UDP, ICMP or the transport layer source or destination ports.
Packet filtering firewalls are low cost, have just a little effect on the network performance, and do not need client computers to be configured in any particular way. On the other hand, packet filtering firewalls are not considered to be especially protected on their own because they do not recognize application layer protocols. Consequently, they cannot take content-based decisions on the packets, which makes them less secure than application layer and circuit level firewalls. One more drawback of Packet filtering firewalls are they are stateless and do not keep the state of a connection. They also have very small or no logging ability which makes it hard to notice if the network is below attack. Testing the allowance and deny rules is also hard which can depart the network vulnerable or incorrectly configured [IT04b]. Figure 2.9 shows packet filtering.

![Packet Filtering Diagram]

2.8.3.2 Circuit Level Gateways
Nearly 1989-1990, Dave Presotto and Howard Trickey of AT&T Bell Labs established the second generation of firewall architectures with research in circuit relays which were called circuit level gateways [IT04a]. Circuit level gateways are used for TCP connections to monitor handshaking between packets to make sure a demanded session is legitimate. Usually, it would accumulate the following information: an exceptional session identifier, the state of the connection (i.e., Handshake established or closing),
sequencing information, source or destination IP address, and the physical network interface through which the packet arrives or leaves.

The firewall then ensures to see if the sending host has authorization to send to the destination, and that the receiving host has authorization to receive from the sender. If the connection is adequate, all packets are routed through the firewall with no more security tests. The advantages of circuit level gateways are that they are generally quicker than application layer firewalls because they execute less evaluation and they can also guard a network by blocking connections between particular Internet sources and internal hosts. The major drawback to circuit level gateways are that they cannot limit admission to protocol subsets other than TCP and likewise to packet filtering, testing the grant and deny rules can be difficult which can go away the network vulnerable or incorrectly configured[IT04c], Figure 2.10 shows circuit level gateways.

![Figure 2.10 Illustrates Circuit Level Gateways](image)

2.8.3.3 Application Level Gateways

The third generation of firewall architectures called application level gateways were autonomously researched and developed during the late 1980s and early 1990s mostly by Gene Spafford of Purdue University, Marcus Ranum, and Bill Cheswick of AT&T Bell Laboratories[IT04a]. Application level gateways or proxy firewalls are software
applications with two main modes (proxy server or proxy client). When a user on a reliance network needs to connect to a service on an untrusted network such as the Internet, the request is directed to the proxy server on the firewall. The proxy server acts to be the actual server on the Internet. It ensures the request and decides whether to permit or deny the request based on a set of rules. If the request is permitted, the server passes the request to the proxy client, which communicates the actual server on the Internet. Connections from the Internet are through to the proxy client, which then bypasses them on to the proxy server for delivery to the real client. This technique guarantees that all incoming connections are for all time made with the proxy client, whilst outgoing connections are always made with the proxy server. As a result, there is no direct connection between the trusted and untrusted networks. The major benefit is that application level gateways may set rules based on high-level protocols, preserve state information about the communications passing through the firewall server, and can keep detailed activity records. The major drawbacks are its complex filtering and access control decisions may necessitate significant computing resources which can cause performance delays and its vulnerability to the operating system and application level bugs [IT04d]. Figure 2.11 illustrates application level gateways.
2.8.3.4 Stateful Multilayer Inspection Firewalls
Verification Point Software released the first marketable product based on this fourth generation architecture in 1994 called stateful multilayer inspection firewalls [Com04]. Stateful multilayer examination firewalls offer the most excellent security of the four firewall types by monitoring the data being communicated at application socket or port layer as well as the protocol and address level to validate that the request is performing as anticipated. Such as if during an FTP session the port numbers being used, or an IP address were to vary, the firewall would not permit the connection to carry on.

An additional benefit is when an explicit session is complete; any ports that were being used are closed. Stateful inspection systems can dynamically open and close ports for every session which vary from basic packet filtering that leaves ports in a steady opened or closed state. The major drawbacks to stateful multilayer examination firewalls are that they can be costly because they necessitate the buy of supplementary hardware and/or software that is not usually packaged with a network device [Inf04] [Vic04], Figure 2.12 shows stateful multilayer inspection.

![Figure 2.12: Illustrates Stateful Multilayer Inspection](image)

2.9 TRUSTED SYSTEM CRITERIA
A trusted system is a computer and operating system that can be established to implement a given security policy. Usually, the focus of a trusted system is data access control. A
policy is implemented that dictate what objects may be accessed [HP01]. The ability of
the system can be improved to protect against intruders and malicious programs by
implementing trusted system technology. There are lots of characteristics:

1. **Functional correctness:** the program does what it is supposed to, and it works
   properly.

2. **Enforcement of integrity:** even if introduced erroneous commands or commands from
   unauthorized users, the program continues the correctness of the data with which it has
   contact.

3. **Limited privilege:** the program is permitted to access secure data, but the access is
   minimized. In this neither the access rights nor the data which are passed along to other
   untrusted programs or back to an untrusted caller.

4. **Appropriate confidence level:** the program has been studied and charged at a degree
   of trust suitable for the type of data and environment in which it is to be used. Trusted
   software is frequently used as a secure way for common users to access sensitive data.
   Trusted programs are used to perform restricted (safe) operations for users without
   allowing users to have direct access to sensitive data [Bel00].

2.10 INTRUDERS

One of the most exposed threats to security is the intruder, intruders may be human
attackers who are able to gain unauthorized access to computer resources or computer
program (e.g., Trojan horses) that appear to be useful, but secretly attack a system or a
resource. A program which contains viruses can act as intruders too [SHP11]. Anderson
[And80] recognized three types of intruders: *Masquerader* is probably to be an outsider,
*Misfeasor* mostly is an insider, and clandestine user can be either an outsider or insider.
Figure 2.13 illustrates attack sophistication vs. Required intruder knowledge.
2.10.1 Intrusion techniques

The purpose of the intruder is to gain access to a system or to enlarge the range of privileges available on a system. Mainly initial attacks use system or software vulnerabilities that permit a user to execute code that opens a back door into the system. Intruders can acquire access to a system by exploiting attacks such as buffer overflows on a program that runs with certain privileges. Figure 2.14 illustrates the number of intruders capable to execute attacks. The intruder attempts to obtain information that must have been protected. In several cases, this information is in the form of a user password. With knowledge of a few other users' passwords, an intruder can log in to a system and work out all the privileges accorded to the valid user [Sta11]. The main ways by which an attacker can get into the system are as follows:
1. **Physical intrusion:** this way of intrusion supposes that an attacker has physical access to a machine. In such case, the attacker has the ability to physically take apart the system and remove the disk drive (and read / write it on another machine).

2. **System intrusion:** this way of hacking supposes that the attacker previously has a low-privilege user account on the system. If the system does not have the most recent security patches, there is a good chance for the attacker to gain extra administrative privileges.

3. **Remote intrusion:** this way of hacking occupies those attackers who do not have any unique privilege and still attempt to break throughout a system remotely across the network. There are some forms of this type of hacking. Network intrusion detection systems are mainly concerned with remote intrusion [SHP11].

![Number of Intruders Able to Execute Attacks](2004 by Carnegie Mellon University)

**2.11 CHAPTER SUMMARY**

In this chapter we explain introduction to network security and literature review for historical network security we refer to some basic network security attacks also include two types of network security attacks: passive attacks and active attacks. We explain security services improve security of data processing systems and information transfers
of an association and meant to contradict security attacks. We explain security mechanisms can be divided into two classes: specific security mechanisms and pervasive security mechanisms. Also, explain malicious software that means intruder to take over or damage a target host without the owner’s consent and often without his or her knowledge and they are different types of this software. We described distributed denial of services attacks and defense mechanisms and explain denial of services attacks as an attack designed to render a computer or network incapable of providing normal services, include: types of DoS and DoS defense problems. We explain a firewalls is a piece of software or hardware that filters all network traffic between a protected or “inside” network and a less trustworthy or “outside” network. Firewalls implement security policies which distinguish “good” traffic from “bad” traffic include: features, firewall design principles, and there are four types of firewall: packet filtering, circuit level gateways, application level gateways, and stateful multilayer inspection firewalls. We described trusted system criteria is a computer and operating system that can be verified to implement a given security policy. One of the most publicized threats to security is the intruder, intruders may be human attackers who manage to gain unauthorized access to computer resources or computer program (e.g., Trojan horses) that seem to be useful, but secretly invade a system or a resource. The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system. Hence, in developing network security system is to know what will protect, because the accurate knowledge of the protected environment provide the preemptive security measures, and enable detecting threats. Generally all attacks follow a general life-cycle to bypass the many layers standing between the attacker and its victim. Intrusion a network is not a simple operation; it passes by different techniques and layers.