Chapter 5

Denial-of-Service Attack

5.1 Introduction

Denial of Service attack is the major threat to the networks, computers and communications systems today .They have negatively affected services to organizations, individual users, critical Internet infrastructures etc., over the past decade or so [23]. *DoS Attack* (including DDoS) is a malicious attempt to disrupt, degrade or prevent the availability of an Information resource to the legitimate users. The resources here are disk space, CPU time, the network bandwidth, memory and other structures like static memory or memory buffers [71]. 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 *Degrading (non-destructive) DoS attack*. A DoS attack can be executed from single source or from multiple sources 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.

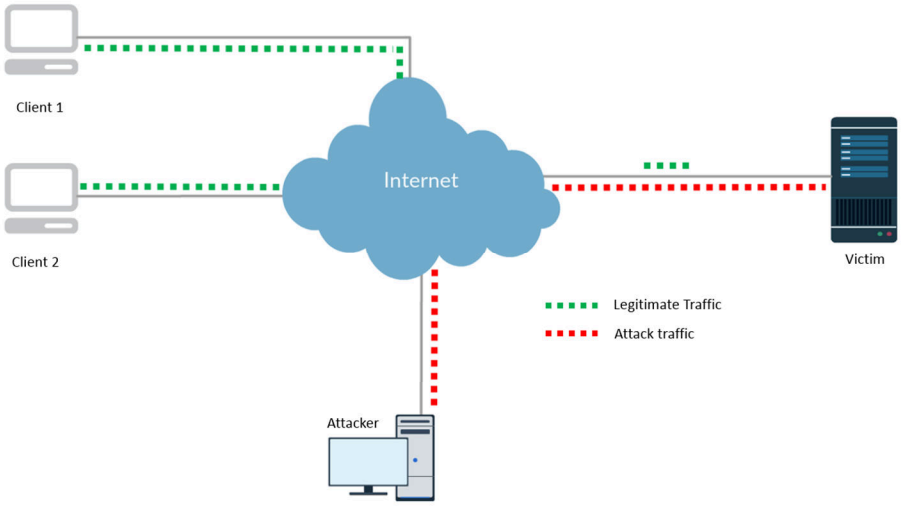

Figure 5.1: Denial-of-service attack plot.

Figure 5.1 illustrates a common DoS attack scenario in which an *Attacker* (attack machine) sends large number of malicious packets to the *Victim* computer. Because of this attack the

legitimate clients *Client 1* and *Client 2* are denied service from the Victim machine. An attacker always keeps itself anonymous and controls some other machine for their work or uses a forged identity, so most likely the attacker machine here is not the real attacker machine but is an *agent machine* recruited by the Attacker.

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. 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 from multiples sources is called as *Distributed denial of service attack (DDoS). A DDoS* attack traffic usually comes from a large number of compromised hosts.

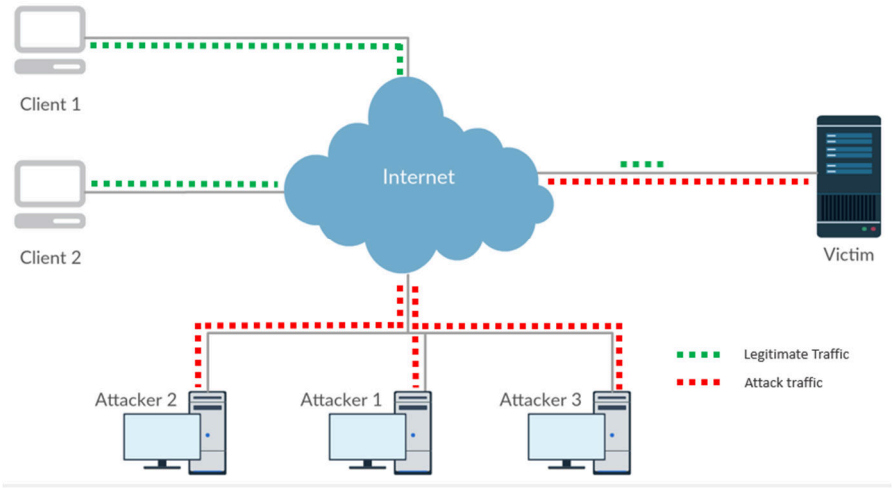

Figure 5.2: Distributed denial-of-service attack plot.

These attack packets arrive at the victim in such huge numbers that some critical resources like CPU time, network bandwidth, memory buffers etc. are exhausted is a rapid manner. The huge number of packet arrival either crashes the victim or keeps the victim busy handling the traffic so that the legitimate users are deprived of the service provided by the victim machine. The legitimate clients are deprived as long as the attack lasts. Figure 5.2

illustrates a common DDoS attack scenario in which the attacker machines *Attacker 1, Attacker 2* and *Attacker 3* send large number of malicious packets to the *Victim* computer. Because of this attack the legitimate clients *Client 1* and *Client 2* are denied service from the Victim machine. 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)* 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 a main controller (the attacker), masters and agents organised in a structured way i.e. hierarchically is referred to as the *Botnet* [132]. The Botnet is controlled by the owner using a software called as Command and Control (C&C) [133]. Figure 5.3 gives us the large scale DDoS attacks (above 300 GBps) by 5 lethal botnets recorded since 2014.

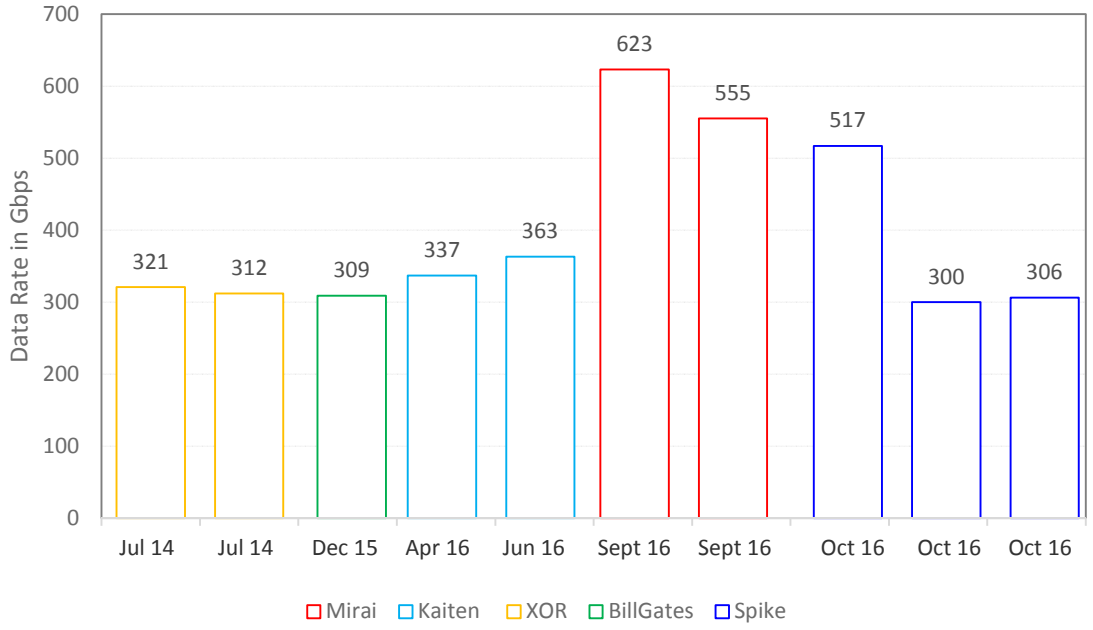

Figure 5.3: 5 lethal botnets in action in recent years[1].

[1] State of the Internet Security Spotlight [140].

5.2 Modes of Operation

DoS attacks (single and multiple source) are very easy to orchestrate and bring havoc to the target machine, reason being the simplicity in design and user interface, without requiring any significant knowledge or expertise or resource for their functioning. The attack tools are readily available on the Internet especially on Deep and Dark web [134]. The motive of the attack (resource exhaustion) is achieved by generating malicious traffic towards the victim in large numbers. The scale of traffic generated is what differentiates the single source and multiple source DoS attacks. DDOS attacks make use of large number of compromised machines in a coordinated fashion, due to which they are more reckless than a single source DoS attack.

Single source DoS Attack: Once the *DoS* attack tool is downloaded and installed on the attacker machine, the attacker is just two steps away from bringing havoc to the target machine. The step before launching the attack is to configure the attack tool for the attack. The commonly required configuration is the destination *host-name* or an *IP-address* and masquerading the attacker identity. Once this is done the attacker is all set to unleash hell on the target machine in the form of flooding or a logic attack. Figure 5.4 illustrates the most common attack structures used by DoS and DDoS attackers.

Multiple source DoS Attack (better known as DDoS): A DDoS attack has several stages. The first step by the attacker is to recruit the *slave (agents/zombies)* machines. This process is done automatically through a *control channel.* The attacker accomplishes this by using a vulnerability scanner tool. The scanner tool is deployed on another compromised machines called as *masters (handlers)*. Random remote machines are scanned for vulnerabilities, and the machines with security holes present in them are exploited and then infected with the attack code by the attacker. The infected machines are then used to attack the target machine. The Agents machines in the botnet are always kept undercover. Any log related and any other evidence that could lead to suspicion is destroyed. The attack scripts installed on masters and agents are kept hidden under system directories and renamed to system file like names for providing anonymity from the user attention.

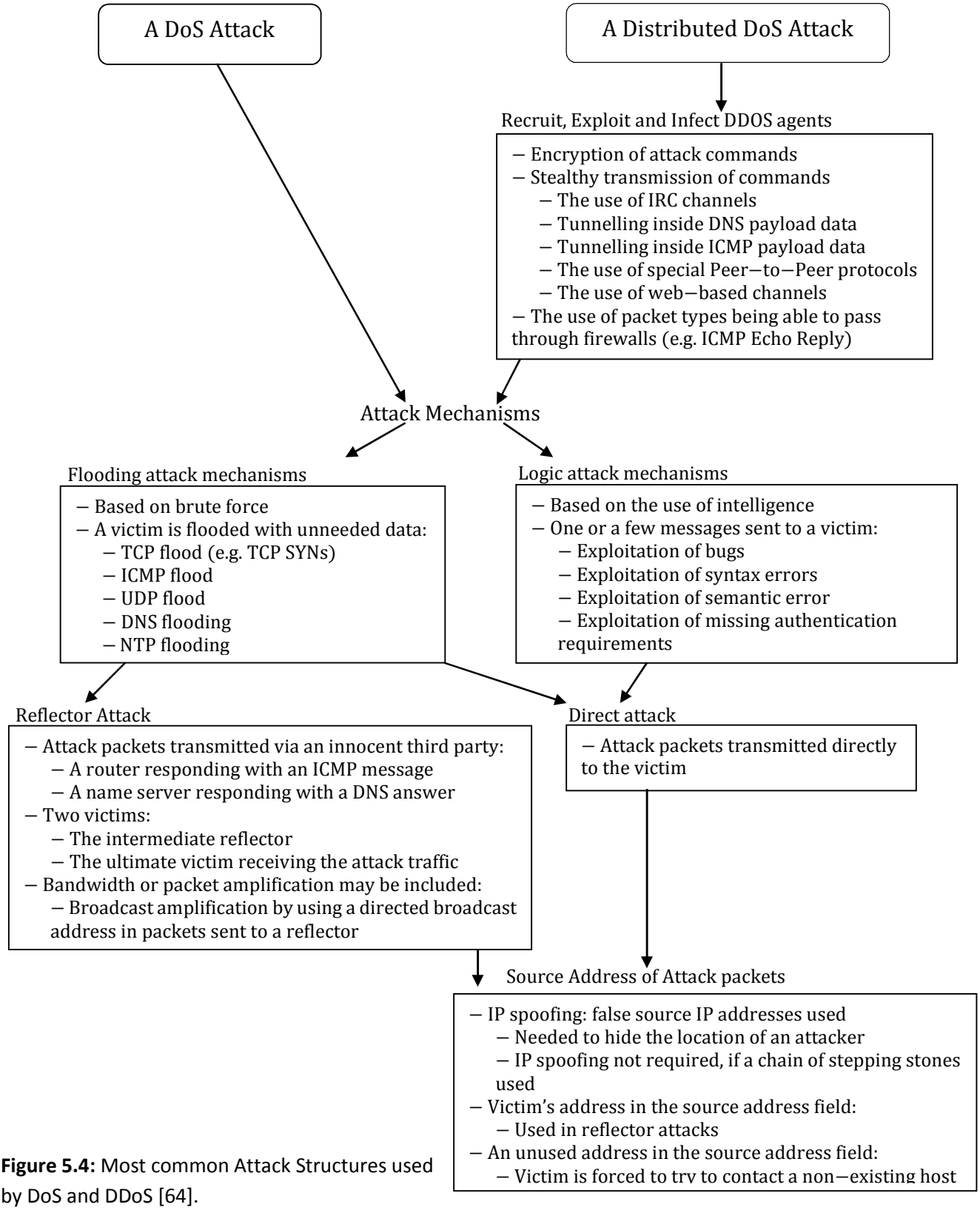

Figure 5.4: Most common Attack Structures used by DoS and DDoS [64].

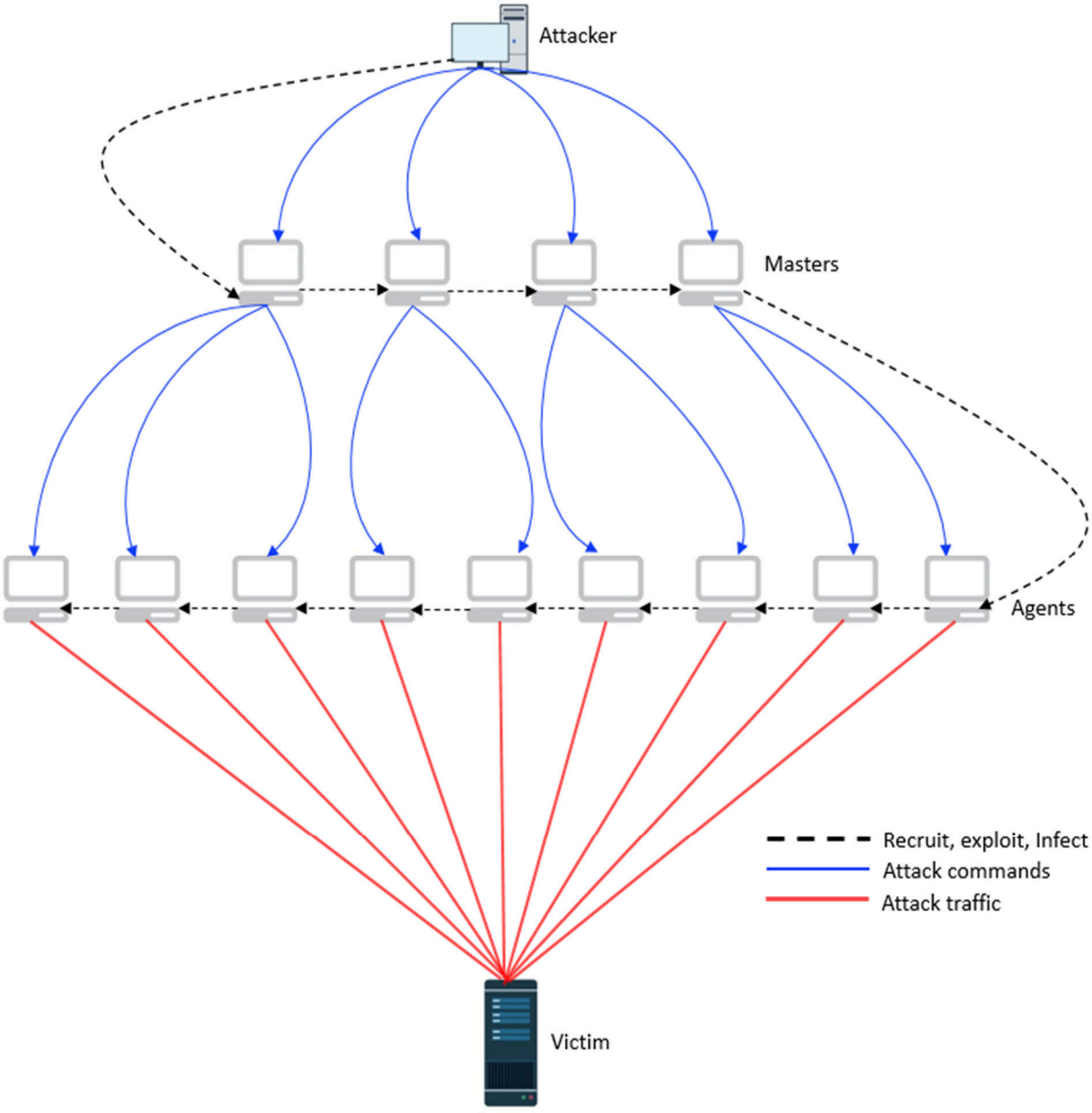

Figure 5.5: Steps in Coordinating a DDoS attack.

There is also a risk of a machine being taken over by other hackers, a professional attacker takes care of all these things and disrupts services at will without any fear of being caught. During a DDoS attack, agent machines are controlled and commanded to send the attack packets to the victim. The attacker coordinates the onslaught of the attack, and plot details

such as the desired attack type and period and the target address from the master to the agent machines. Agent machines usually fire out the packets at a maximum possible rate to increase the attack's chances of success. However, there have been attacks where agents were generating packets at a small rate (to prevent agent discovery) or where agent machines were periodically pausing the attack to avoid detection (*pulsing attacks*) [138]. The whole process of recruitment, exploitation and injection of the attack code is automated and carried out using *command and control* software. The most widely used control channels are the IRC channels [135,136], but in the last decade or so various botnets have shown an increasing trend in the usage of web based channels for control and coordination of the attack. The slapper worm [137] coordinates the traffic over peer-to-peer networks. Certain tools have incorporated tunnelling to bypass security mechanisms for the control and coordination of the attack [17]. Figure 5.4 illustrates the most common attack structures used by DDoS attackers. Figure 5.5 depicts the process of recruiting, exploiting, infecting and the engagement of the compromised hosts, the figure also illustrates the master/slave architecture of the Botnet/compromised hosts.

5.3 Frequently Observed Attacks

There is a vast majority of Denial of Service attacks that are happening everyday throughout the year [23], the most frequently observed attacks during the majority of DoS attack incidents are as follows:

5.3.1 UDP flooding attack

A large number of UDP packets are sent towards the victim so that the network bandwidth of the victim is full with the malicious traffic and no bandwidth is left for legitimate service requests to the victim machine. The goal of this attack is just to make the victim process an extremely huge amounts of data. In order to fully render the network services un-available large sized packets are used in the attack. This attack is very easy to carry out, we just need a victim address and a specified or a random port number. Usually attack is carried out on random port numbers of the target machine. Attack can be launched from

single source or from distributed sources (DDoS) using multiple agents. Using a large number of multiple agents will ensure a successful attack. This attack can be avoided by using simple filtering rules at high bandwidth points in a network (i.e. upstream router) [19 and 138]. Figure 5.6 gives us an idea about UDP flooding attacks in the recent years. The values indicate a percentage out of the total number of security incidents observed [144] during the said period by Akamai Technologies[2] and Arbor Networks [23].

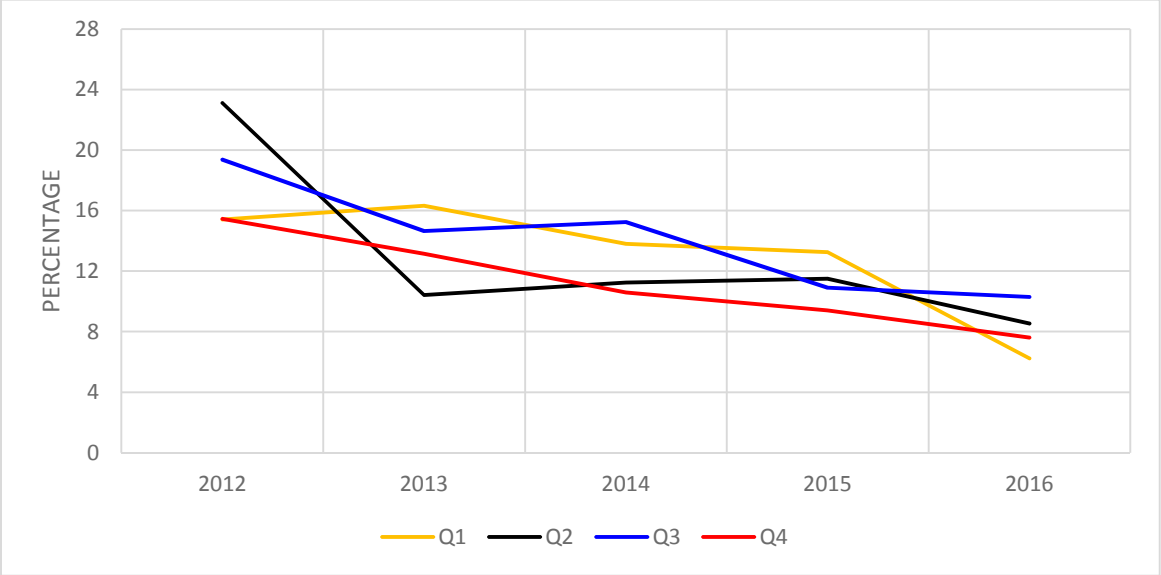

Figure 5.6: State of UDP flooding attacks in recent years.

5.3.2 ICMP flooding attack

ICMP protocol gives us a feature in networking to check whether a remote computer is alive or not by sending an ICMP_ECHO_REQUEST packet towards the remote system. In case of ICMP flooding attack a large number of malicious ICMP_ECHO_REQUEST packets are directed towards the victim. Upon receiving the requests the victim starts replying to each and every request, due to which the resources of the victim, CPU, memory

[2] Akamai's content delivery network is one of the world's largest distributed computing platforms, responsible for serving between 15 and 30 percent of all web traffic.

and network resources are consumed. Again just like the UDP flooding attack, this attack can be carried out from single sources and multiple sources using agent machines.

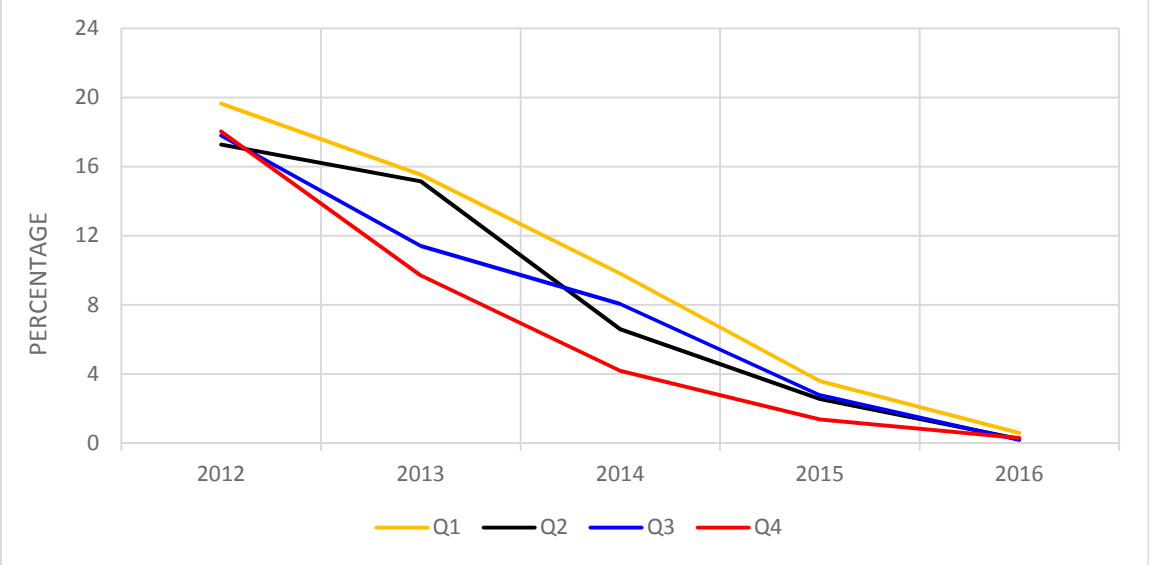

Figure 5.7: The decline of ICMP flooding attacks in recent years.

During a DDOS ICMP flood attack the agents generate huge and gigantic volumes of ICMP_ECHO_REPLY packets (ping) towards the victim and forcing the victim to reply to such a large number of requests. Normally to avoid this situation a rate-limiting rule at a high bandwidth point is used [78 and 139]. Figure 5.7 presents the state of ICMP flooding DoS attack is recent years, as observed in [144], the figure shows a declining trend in the last 5 years.

5.3.3 NTP Amplification

Since its introduction in 2012 (strong attacks started in late 2013), the DoS attacks using Network Time Protocol (NTP) amplification are up on the rise and progressively more common than ever before [141]. The NTP Protocol is used to synchronize system clocks and used to deliver accurate time to networked hosts on internet. For the purpose there are dedicated NTP servers scattered all over the internet. We have a UDP based command 'MONLIST' which if called returns a list of last 600 connections (IP addresses) from the

NTP server. MONLIST requests are sent out by Attackers to the NTP servers using a target server's spoofed IP address and needless to say the NTP server responds with gigantic UDP packets to the spoofed IP Address. When requested for the recent list of clients he NTP server responds in up to 100 UDP datagrams with 440 bytes of payload each. It has been observer that on average the request gets amplified by a factor 556.9 – 4670.0 [143]. Since this attack is a DDOS attack, the first step is the recruitment step. Vulnerable hosts are scanned on internet and recruited. In early 2014 there were more than 430,000 such vulnerable NTP servers [141]. The recruited host is called as an amplifier. Amplifiers job is to amplify the request it receives into huge UDP packets in large numbers. An amplifier is simply a host running a protocol (e.g., NTP, DNS) which, when sent a query packet, responds with one or more packets whose aggregate size is larger than the query it received. Once the hosts have been identified through the control channels, the attacker send in small UDP datagrams with spoofed source IP address of the victim machine and the address of the recruited amplifier as the destination address.

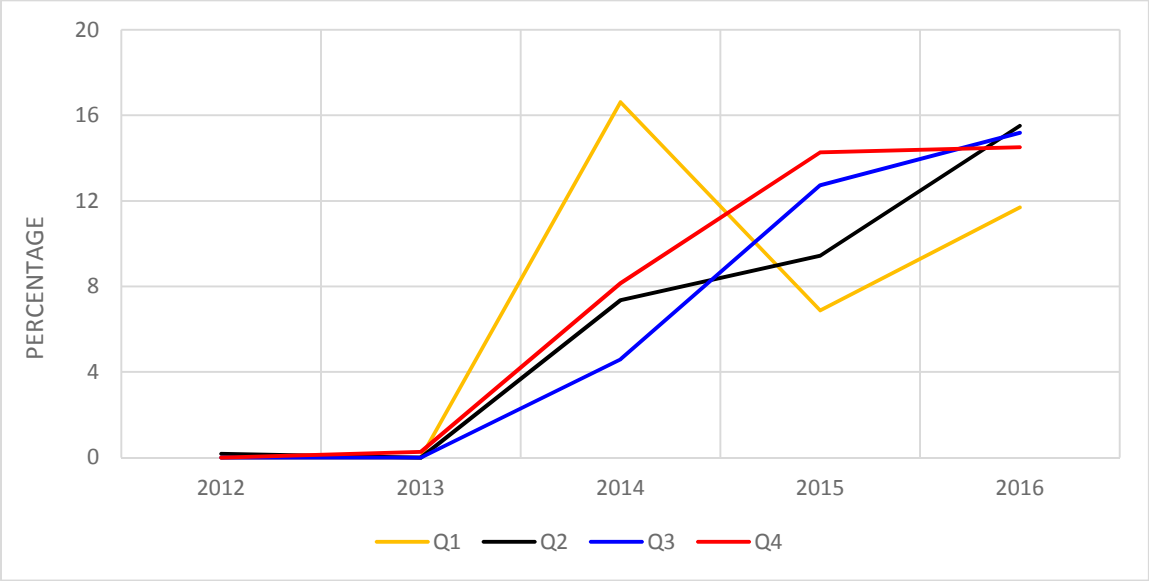

Figure 5.8: The rise of NTP Amplification attack since its inception.

This results in large amounts of traffic from the amplifier, which may consume all the network bandwidth at the victim site. Therefore a command which was intended only for

diagnostics, returns the last 600 clients of the amplifier, producing a typically very large, multi-packet reply to a single small query packet—an ideal amplification attack vector [142]. Figure 5.8 gives us an idea about NTP amplification attacks in the recent years. The values indicate a percentage out of the total number of security incidents observed [144] during the said period by Akamai Technologies[3]. The plot shows an alarming trend in the attack as since its inception, it's increasing and increasing at an alarming rate. By April 2014, data by the *ARBOR Networks*[4] reports showed that 85% of DDoS attacks above 100 Gbps were using NTP amplification [141].

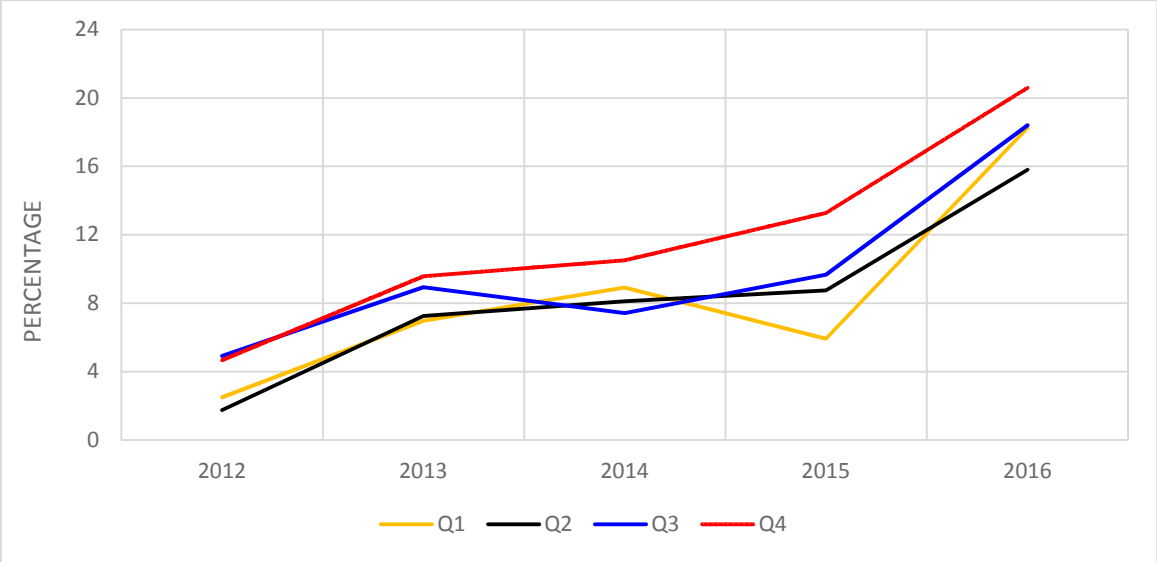

Figure 5.9: DNS amplification attack in recent years

5.3.4 DNS reflector attack

In a typical scenario the attacker forwards a Domain Name System (DNS) query packet (which is also known as DNS lookup) to a DNS server. The attacker spoofs the IP address field of the packet with the victim system IP address. Upon handling the request and processing it the DNS server responds back with a reply. When the response reaches the

[3] Akamai's content delivery network is one of the world's largest distributed computing platforms, responsible for serving between 15 and 30 percent of all web traffic.

[4] Arbor Networks is a company which specializes in DDoS attack Defence , the data has been collected From more than 287 ISP's worldwide.

victim, the victim will process it and simply discard it as the original source of the packet was someone else. During this process some of the victim's resources were consumed. The response packet is much larger than the query packet. Now just imagine when the responses come from thousands of such DNS servers in a distributed and coordinated fashion, the victim is bound to suffer. The victim's resources are consumed within no time. The DNS amplification attacks are on steep rise since 2014 [144], as evident from the figure 5.9.

5.3.5 TCP-SYN flooding attack:

The most extensively used DoS attack is TCP SYN flooding attack. Majority of the DoS attack tools support this type of DoS attack and also various studies give an indication that majority of the DoS attacks abuse the TCP protocol [73].

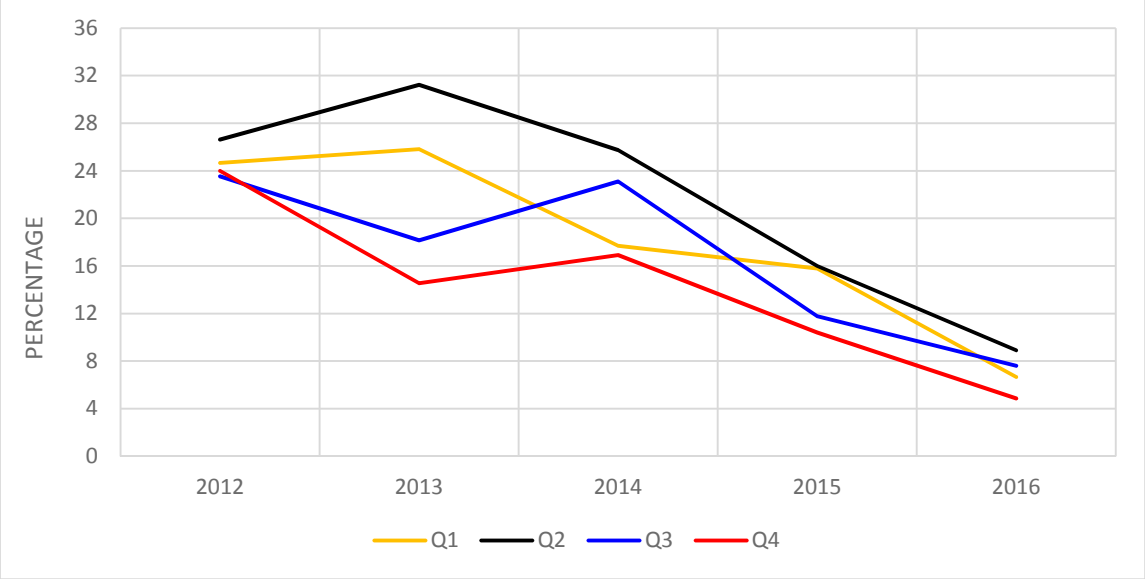

Figure 5.10: State of TCP SYN flooding attack in recent years.

The reason for such hostility against the TCP protocol is the flaw in the TCP protocol design. The attacker exploits the three way TCP handshake process by creating a huge number of legitimate half open TCP connections. A more detailed discussion on the issues in the TCP protocol and the remedy is carried out in the next section. Figure 5.10 showcases the declining trend in the TCP SYN flooding in the internet in recent years and 2016

contains the lowest recorded percentage at around 5% of the total internet security issues that occurred worldwide, but 5% is also a huge number when we consider all the security incidents that occurred in the same year .

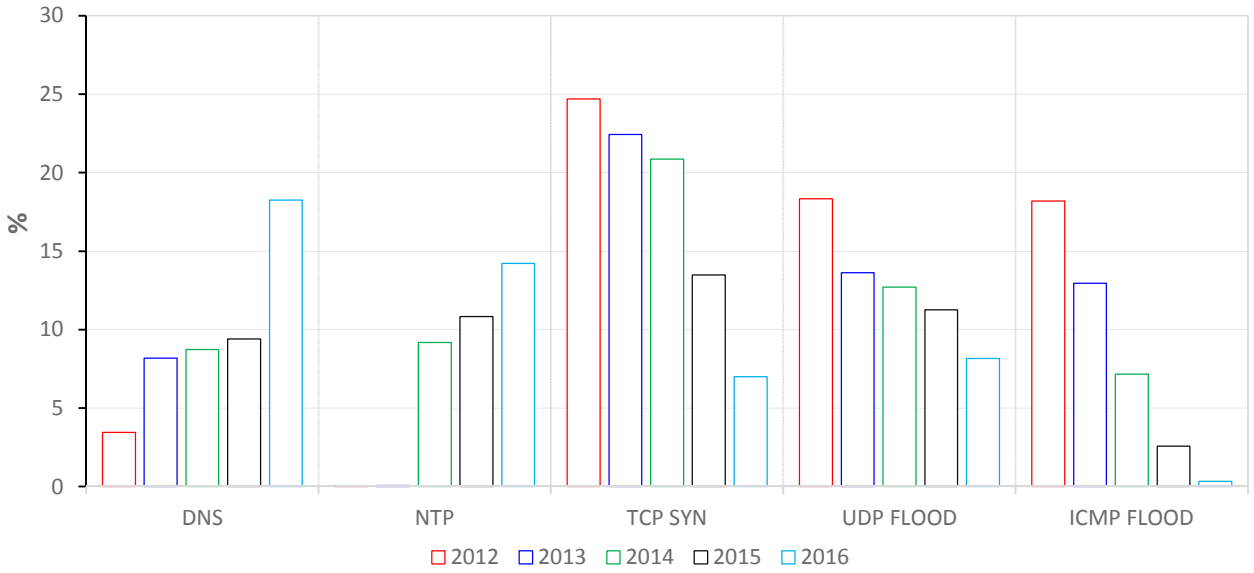

Figure 5.11: Analysis of the well-known DoS attacks since 2012.

5.4. Conclusion

After discussing and analysing the frequently occurring DoS attacks in the recent years (2012-2016), we found TCP-SYN as the most frequently occurring DoS attack, followed by UDP flood, DNS amplification, ICMP flood and the newly rising NTP amplification. The amplification attacks showed a steep increasing trend in the recent years and continue to dominate to be the most devastating form of DoS attacks (distributed in nature) on the internet present today. All the others (ICMP, UDP and TCP SYN flooding attacks) on average show a downfall of around 20% between the periods 2012-2016. Figure 5.11 sums up the story of DoS attacks in recent years.