Amanda Lewis

Mr. Moe

COSC 3344

8 March 2019

DDoS Attacks

The world is becoming more and more connected as we speak. Many people enjoy using the internet, as well as IoT devices to make their lives easier and smart homes or other smart grids to make their homes smarter and more secure. But all this can backfire when they become a victim of a DDoS type attack, causing a depletion of resources and bandwidth. These attacks may be done for financial gain, personal revenge, an ideological belief, an intellectual challenge, or in the name of Cyberwarfare, where one country attacks another country's infrastructure. In this paper I will be talking about the effects of DDoS attacks, the different type of DDoS attacks, and intrusion prevention intrusion detection strategies for managing these attacks.

A general DDoS attack involves an attacker recruiting attack armies. First they find IP addresses and computers to act as the "masters" that scan for "slave" computers to use. All these computers have in common is that they have security loopholes that allow them to be taken advantage of. Sometimes these computers in the attackers army are IoT devices with terrible security protocols.

There are three phases to a DDoS attack, recruiting, as I have mentioned above, propagation, which is passing the attack codes onto the "slaves", and the attack phase. During the attack phase, attackers have the choice of either doing a resource depletion attack, or a bandwidth depletion attack. A resource depletion attack either involves sending deformed packets, or by exploiting some network, transport, or application layer protocol to achieve their goals. Among the protocols that can be used are TCP, HTTP, and SIP.

There is the TCP SYN attack, where the attacker exploits the three-way handshaking protocol of TCP's connection creation process. In this attack, the attacker sends multiple spoofed SYN packets, and the victim sends a SYN + ACK package back, and expects to hear a final ACK packet which finishes the handshaking process. The victim will hold on to all of the intermediate states in the memory stack, but when none of the handshakes are ever completed, the memory stack begins to fill up fast because of the large number of incomplete connections. Thus, genuine users who want to connect to the victim will not be able to and will be forced out of the system.

The second type of attack that exploits the TCP protocol is a TCP PUSH + ACK attack. For this type of attack, the attacker sends a large number of TCP packets and set "1" to the PUSH and ACK bits of the header, which means the victim must clear their memory stack to send an acknowledgement to the client, and this eventually leads to the processing power and memory overload to run out.

The next type of attack assaults the HTTP protocol in the application layer. In this kind of attack, the attacker manipulates HTTP get and post requests while talking to a server. This requires the attacker to set up a TCP connection with a valid IP address in order for the attack to work. Another similar type of attack is the SIP flood attack, where an attacker makes different types of SIP request messages where the goal is to flood the SIP registration server or proxy server and to use up all its resources.

The last type of protocol-exploiting attacks is the slow request/response attacks. This type of attack slowly consumes resources, while most of the time trying to only use a single computer.

It can be called Slowlories, HTTP fragmentation attack, Slowpost, or RUDY (R. U. Dead Yet?) attacks. The purpose of the attack is to fragment packets down to the minimum packet size and send them as slowly as possible so the connection remains open for a long time, eventually depleting the resources of the computer. This can be prevented by rejecting unsupported HTTP connections or applying a limit on the rate of the incoming data.

A malformed packet attack can be done in many ways. There is the land attack where it sets the victims IP address to the packet's source and destination IP addresses, sending the packet in an infinite loop, which can eventually crash the system. In an IP packet option field attack, they target the optional fields of an IP packet and randomize that information. This causes the processing ability of the victim to fail when too many deformed packets are sent. The ping of death attack involves sending a packet that is over the limit of the maximum packet size, which causes the victims computer to freeze or crash. In a Teardrop attack, the attacker manipulates the offset value, generating errors in fragmentation which then leads to problems trying to re-build those packets, so invalid packets are created causing the host machine to crash or reboot. These attacks constitute all the resource-depletion attacks, and in the next section, we will discuss bandwidth depletion attacks.

A bandwidth depletion attack can also be protocol exploited, where the attacker takes advantage of transport layer protocols such as User Datagram Protocol (UDP) and network layer protocols such as Internet Control Message Protocol (ICMP). In a UDP flood attack, the attacker sends a large stream of UDP packets from the army of bots it has, and since the destination IP address is spoofed, the port will try to identify the type of application that is waiting on the destination port, and when it finds no application is waiting, it responds with an ICMP packet that basically reads, "destination unreachable".

In an ICMP flood attack, the IP layer is exploited with ICMP's ICMP_ECHO_REQUEST packets. This is normally used to check whether a remote host is alive or not, but in DDoS attacks, the attacker sends the packet using a broadcast address of all 1's, and so it is delivered to all machine's in the victim's network.

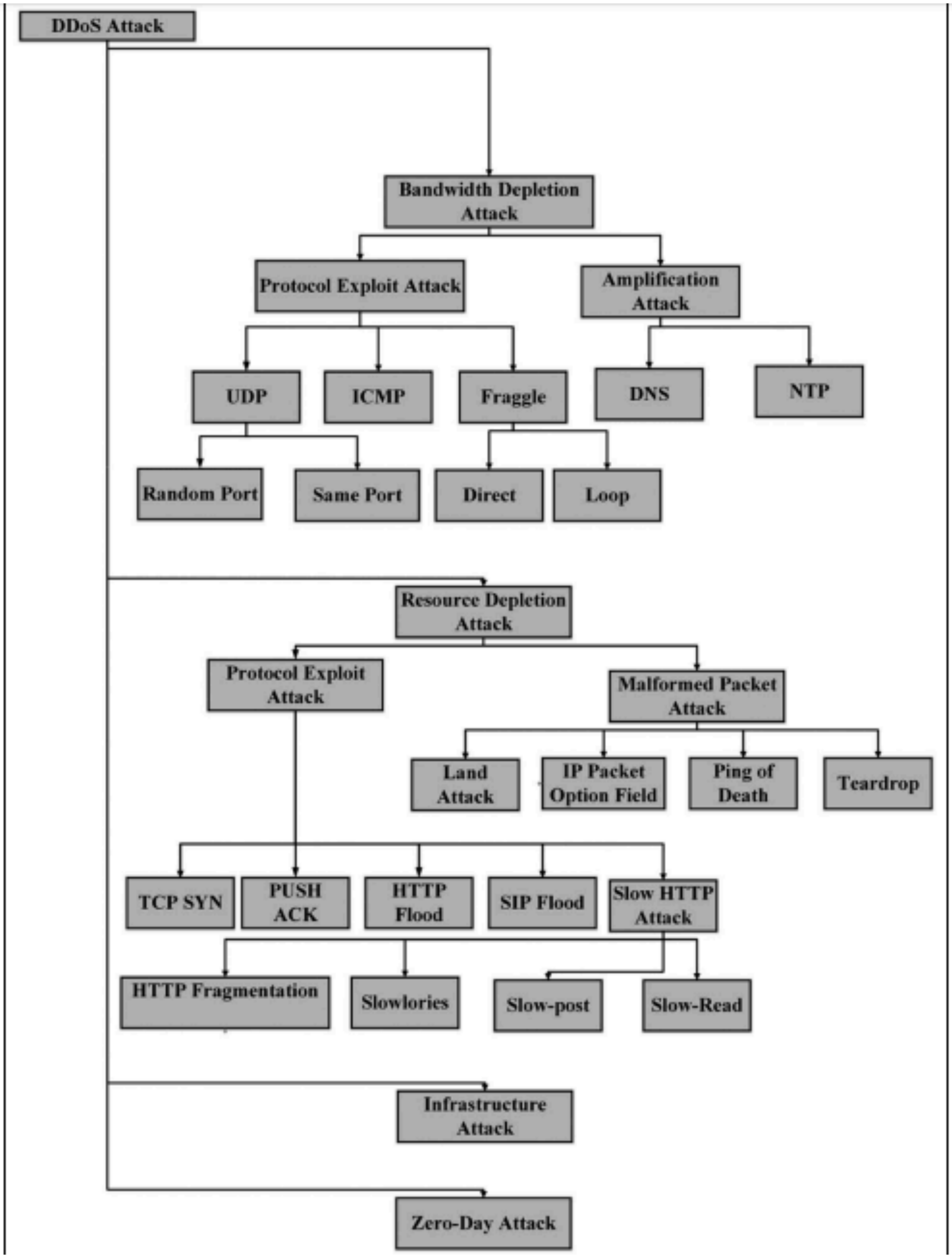
Another type of attacks, called amplification attacks, generate a large response for a small request and direct the responses at a victim. The most common types are DNS amplification attacks, which is an example of a reflection attack. This type of attack uses multiple DNS recursive servers to send a large number of UDP packets to oversaturate a victim while sending reflected responses to the spoofed source/victims IP. Then there is the NTP amplification attack, which is similar to DNS amplification attack and it exploits NTP instead of DNS.

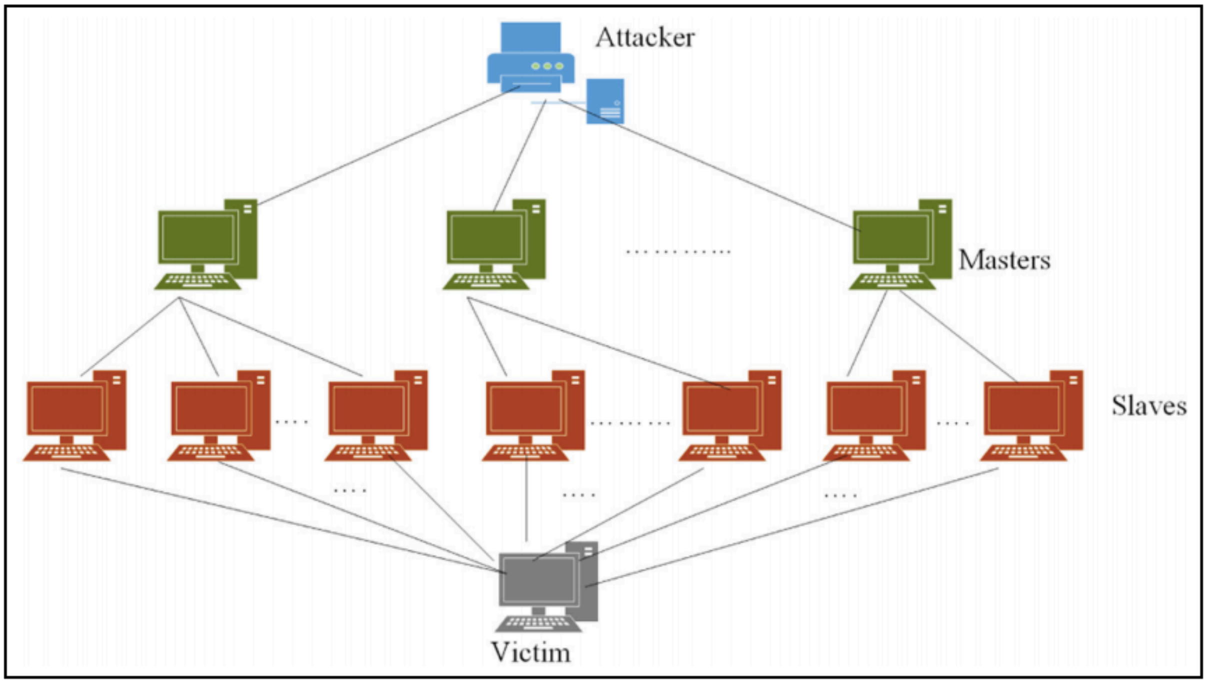
The combination of a resource depletion attack and a bandwidth depletion attack is an infrastructure attack, or one that targets both. The goal of the attack is to damage crucial elements of the internet, so it targets the bandwidth of the network but also the resources of the targeted system. Many infrastructure attacks take place with the help of smart devices and IoT that people do not realize are infected and part of a botnet for some time. The last type of attack is called a Zero-day attack, because the security vulnerabilities are not known until day 1 after the attack. The attack takes place on day 0.

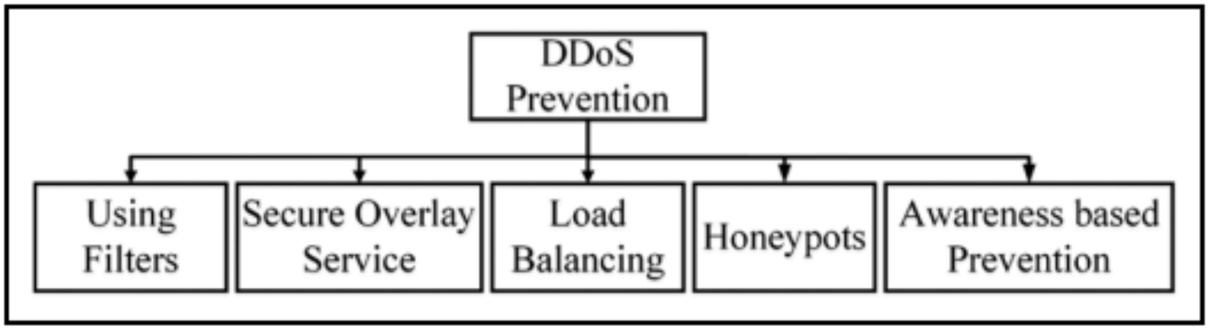
There are many ways to attempt to prevent DDoS attacks. You can use filters to filter out malicious traffic, which helps detect spoofed IP addresses, but if the valid IP addresses of the botnets are used, then filtering will not work. Then comes secure overlay, where an overlay network is built on top of the IP network. The overlay network acts as a bridge/entry point for the outside network to establish a connection with the protected network.

Lastly, honeypots are another great way to ward off DDoS attacks. Honeypots/nets are a great way to attract attackers to break into a less secure system, while keeping the main system safe and secure. The "victim" of the honeypot attack can then find out information about the attacker, such as tools, and software used for an attack, though if a honeypot cannot detect an attack using its detection tools, then the malicious packets are forwarded onto the real destination. There are many more ways to detect and prevent DDoS attacks.

In conclusion, a DDoS attack can be many computers working together to create an army, or it can be one computer in the case of the Slowlories attack. Either way, DDoS attacks are becoming more and more prevalent in our lives, and we need to find ways to detect and prevent these attacks before any major attack happens. Whether it be a resource depletion attack, a bandwidth depletion attack, or both, with an infrastructure attack, our networks need to be prepared.


DDoS Attack
Bandwidth Depletion Attack
Protocol Exploit Attack
Amplification Attack
UDP
ICMP
Fraggle
DNS
NTP
Random Port
Same Port
Direct
Loop
Resource Depletion Attack
Protocol Exploit Attack
Malformed Packet Attack
Land Attack
IP Packet Option Field
Ping of Death
Teardrop
TCP SYN
PUSH ACK
HTTP Flood
SIP Flood
Slow HTTP Attack
HTTP Fragmentation
Slowlories
Slow-post
Slow-Read
Infrastructure Attack
Zero-Day Attack


Attacker
Masters
Slaves
Victim


DDoS Prevention
Using Filters
Secure Overlay Service
Load Balancing
Honeypots
Awareness based Prevention

Hmood, H. S., et al. “Adaptive Caching Approach to Prevent DNS Cache Poisoning Attack.” *The Computer Journal*, vol. 58, no. 4, 2014, pp. 973–985., doi:10.1093/comjnl/bxu023.

Lohachab, Ankur, and Bidhan Karambir. “Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks.” *Journal of Communications and Information Networks*, vol. 3, no. 3, Sept. 2018, pp. 57–78., doi:10.1007/s41650-018-0022-5.

Mahjabin, Tasnuva, et al. “A Survey of Distributed Denial-of-Service Attack, Prevention, and Mitigation Techniques.” *International Journal of Distributed Sensor Networks*, vol. 13, no. 12, 2017, pp. 1–33., doi:10.1177/1550147717741463.