ECE8860 DDoS

Final

R. R. Brooks - rrb@clemson.eduApril 2021

Student – Shriya Reddy Surusani

Answer each question clearly and concisely. Each question is worth 12.5 points.

1. The essential Internet flaw that enables DDoS is a lack of access control for the network. Consider an Internet where there is effective access control globally. Answer the following:

- What effect would this have on DDoS attacks?

The number of DDoS attacks observed and the frequency of their occurrence will surely drastically decrease. The reason being, when access control is effectively in place. The attacks can be monitored to trace back to the source of the packets that are being sent by the attacker, easily. Once the sources are tracked (which would most probably be compromised machines of legitimate users). The malware (backdoor to be specific) on the compromised machine can be removed which will make the attacker lose control over the system and also the machines would be no longer a part of the attackers' botnet and hence making any next DDoS attack less probable. The tracing back to the source of the attack packets would be possible because, effective access control globally will leave no room for spoofing during the attack.

- What other effects would this have on Internet use?

One of the most prominent effect would be that internet use will be more secure and safe. Since all the users are authenticated and authorized in this ideal world, every user is accountable and could be tracked. It will be safer and secure to use because the distribution of malware (which is the foundation for carrying out an effective DDoS attack) over the network will be reduced and thus giving out more network bandwidth to the users. The side effect of which would be that, user communications or any type of connections over the Internet will be much faster due to the bandwidth availability.

One downside for it would be that there would be no user privacy. Since, all the activities of the machines connected to the Internet could be tracked.

2. Describe 5 different traffic attributes that are analyzed for early detection of DDoS attacks. Explain the advantages and dis-advantages of using each attribute for accurate DDoS detection. Propose a way of combining at least 2 of those attributes for a faster and more accurate detection of DDoS events. Explain the advantages of the combined detection approach.

Following are the 5 traffic attributes that can be used for early detection of DDoS attacks:

i) Traffic Volume using packet count thresholding: Here, abnormality in the number of packets received is used as a judgement factor for detecting the attack. A threshold value for the number of packets is set,

such that the traffic flow below the threshold is considered normal and anything that goes over the threshold value will trigger an alarm that attack has been detected. This method of DDoS detection is purely based on the packet count during certain time intervals in the traffic.

Advantage:

- DDoS attacks are detected faster. Since, detection is triggered as soon as the packet count at any point of time reaches over threshold value.

Disadvantage:

- The false-positive rate is higher because the abnormal increase in the number of packets can happen due to increase in usage by the legitimate users.

ii) Traffic volume using Data Volume Thresholding: Here, we check for abnormalities in the data volume of the packets in the traffic flow. A threshold value is set taking into consideration the normal amount of data that is expected in the packets over the network. When it exceeds the expected value, an attack is detected.

Advantage:

- It would prove to be very efficient in the cases when an attacker is performing a DDoS attack by sending large volumes of data through the packets to use up the whole network bandwidth.

Disadvantage:

- Not very effective when it comes to detecting other type of attacks such as a flood attack. Where, the attacker just sends a large number of packets over the network irrespective of the data volume in it.

iii) Traffic CUSUM: Here, we calculate the difference between the current and long-term average of the traffic. When the current average increases faster than long-term average of the traffic, the cusum coefficient is increased and the cusum coefficient decreases when the difference between the two averages is small. Now a threshold value is given for the cusum, which when exceeded indicates that, there might be a DDoS attack.

Advantage:

- It does not require training and is more robust to variations in the attack profile.
- The detection accuracy is more and the false-positive rate is lower because network is monitored for a period of time instead of making the judgement too soon.

Disadvantage:

- It takes a long time to detect the attack. Since, the traffic flow in this case is monitored for a long period to detect the abnormalities in the traffic pattern.

iv) Wavelet: Here, we analyze an input signal of the traffic simultaneously in the time and frequency domains and localizes the frequency components of the traffic signal produced in the time. In this case, the attacks can be detected with either high-pass filter or low-pass filter.

Advantage:

- More accurately detects the DDoS attack than the traditional detection and less number of false positives are observed because, it is able to capture complex temporal correlation across multiple time scales with very low computational complexity.

Disadvantage:

- Takes time to report an attack which dismisses the whole point of early DDoS detection.

v) Entropy: Here, we measure the amount of disorder in the observed traffic flow. The entropy change during an attack varies based on observed packet header field. Entropy of the source IP addresses increase during a DDoS attack which can be used to detect the attack.

Advantage:

- It increases the sensitivity of detection to uncover anomalous incidents.

Disadvantage:

- When the detection is based on the entropy, it still needs an efficient algorithm to reduce computational time and memory usage in a high-speed network.

Now, we can combine cusum and entropy for a better detection approach. Here, the entropy module calculates the entropy of a packet header field from the packets in an observation window and the entropy of the source IP address is calculated. The entropy data is then decomposed into its high-pass and low-pass components. Then, the filtered entropy data can be processed using the cusum algorithm and the calculated cusum coefficients are used to detect DDoS attack.

Advantage: It detects attacks with high detection and low false positive rates and gives better detection efficiency than a detection approach using entropy of packet header field without further processing

3. Suggest at least 2 changes to the current set of labs we use in this course that would improve the course and require no hardware modifications. Explain why these changes are needed.

Suggestion 1:

- More number of VMs could be installed for using it as a command & control server that could be assigned separately to each student.

  Reason: Since all the students use the same VM, the python scrips used in the lab have the chance of being modified or corrupted, with no one being accountable for it. Also, the files generated while performing the lab are stored in the VM which is accessible by other students as well. This leaves the scope for plagiarism.

Suggestion 2:

- If not a separate VM, each student should have a separate account in the VM used, with all the tools installed in each account which will be used by them alone.

Reason: All the commands used by the student (some of which are unique to the user to answer the lab questions. Eg: Scapy commands) can be viewed by everyone. Hence, leaving the scope for plagiarism again.

4. How has the pandemic modified computer usage patterns? Has this made DDoS attacks easier or harder? More or less common? Suggest how you would exploit this as an attacker.

It is observed that the pandemic has moved the traditional working of life to a virtual mood. Examples would be, schools shifting the mode of teaching to online via video conferencing software and all the software companies shifting work from office to working remotely. There is an overall change in lifestyle because of the pandemic in the majority of the population, where using computers with internet has become a part of their routine. This gives a perfect opportunity for the attackers to carry out their malicious intentions. How? Well, majority of the population is not technically educated about the computer safety. Now that the number of users are increased, the chances of falling for the malicious bait is more and thus increasing the attackers botnet. Since, the larger the botnet, the easier the attack. DDoS attacks can be easily carried out. Now, large botnet network also means that the attackers could generate huge revenue through minimal initial investment. This will make the DDoS attacks more and more common.

If I was the attacker. I would hide the backdoor payload in the pop-up ads over the internet. The pop-up ads will be such that it would be a easy click bait for the non-aware users. Looking at the stats, the number of users that are unaware of even the basic phishing attacks is alarming, but good for me that this set of population will be easy to lure into clicking the pop-up with hidden backdoor payload. Once the payload is installed in the victim machines. I would have access over them and they would be a part of my botnet that I could use to perform the DDoS attacks. Again, looking at the stats, I would have a pretty large active botnet to use.

5. Predict the evolution of DDoS attacks for the next 10 years. Suggest a legal commercial product design that could profit from this evolution.

Let's look at how DDoS has evolved over time, with the increase in use of technology and rapid increase in its availability to the common public. In the next 10 years, graph of availability of internet and the tech devices to everyone is only going up and up. Which means, the number of users who are technically not sound will only increase that will give more room for the attacker to carry out his DDoS attacks. With the increase in interest and easy availability of information and the DDoS attack kits over the dark web will only make the DDoS attacks more frequent and easier. This is also because the number of script kiddies will increase over time.

Since, in 10 years DDoS attacks will be more prominent and frequent which will create interest in people to know and learn more and would also trigger more research funds around it. One can find a way to provide operational network available for these researches. Most of the researches right now are based on the simulated network which do not provided an accurate result that one can see in the operational network. Hence, if one can find a way to commercially lend the operational network for the research purposes, he would be the most profitable, legally, out of the evolution of DDoS attacks.

6. Which attack tool that we used this semester did you find the most useful and/or interesting? Explain.

Personally, I had fun doing lab 5 which involved attack generation. Though every tool we used had its own purpose, Wireshark and Scapy tools were the most useful and interesting for me. For networking sniffing, I used Network monitor before, were dissecting through the packets over the wire was not possible. I could monitor the network but I couldn't exactly figure out what was getting transmitted. Through wireshark, it was much easier and fun to do that. The first lab regarding just the network sniffing did help in exploring wireshark better that I could use it in the further labs when ever I found it to be required. Using scapy made me fill the gaps between the theoretic knowledge of spoofing the packets for an attack to actually implementing it.

7. Respond to one of the problems posed in Section 4.8 (Page 73) of the textbook.

Question: Outline the importance of attack attribution in enforcing anti-DDoS laws.

One of the main problems of DDoS is its global nature, including the role played by botnets in executing DDoS attacks. Since botnet designs provide bad actors with many ways of hiding their actual locations, the ability of any law enforcement agency to find and prosecute the attackers is compromised. It is easy to plant "false flags" that attribute attacks to other players. Hence, tracing back the attack to an accurate geographic location is crucial in order to determine the severity with which antiDDos laws need to be applied. Such that, we could even analyze the patterns of where the most frequent attacks are generated from to come-up with new and better antiDDoS laws. Getting a right location also reduces the chances of triggering a cyber-war against a wrong country.

8. Your employer wants you to come up with a mitigation strategy for likely DDoS attacks. Summarize the strategy you would propose and explain why it is the best solution for your needs.

Depending on the infrastructure, a DDoS response plan can get quite exhaustive. However, here is what I feel would be a good mitigation strategy for likely DDoS attacks. We can have 4 stages to respond to it. Namely: Detection, Response, Routing, Adaptation.

i)Detection: Here, we need to distinguish the increased legitimate traffic from a DDoS attack. For this the best approach would be to use cusum and entropy-based detection because here, the entropy module calculates the entropy of a packet header field from the packets in an observation window and the entropy of the source IP address is calculated. The entropy data is then decomposed into its high-pass and low-pass components. Then, the filtered entropy data can be processed using the cusum algorithm and the calculated cusum coefficients are used to detect DDoS attack which decreases the number of false-positives and has a good detection efficiency.

ii) Response: Here, one the attack is detected, the malicious packets could be intelligently dropped and the traffic could be absorbed. Such that the network is able to mitigate the attempt at disruption.

iii)Routing: The traffic is routed such that it is broken into manageable chunks preventing DDoS.

iv) Adaptation: Analyzing the attack patterns and adapting to them and changing the detection logic accordingly would make an effective protection service that can harden itself against future attacks.