Advanced Topics in IP Networks
Lecture 11

Lecture by Dr. Anat Bremler-Barr
Typeset by Steven Karas

2018-12-27
Last edited 20:57:19 2018-12-27

Disclaimer These notes are based on the lectures for the course Advanced Topics in IP Networks, taught by Dr. Anat Bremler-Barr at IDC Herzliyah in the fall semester of 2018/2019. Sections may be based on the lecture slides prepared by Dr. Anat Bremler-Barr.

1 HW4

published, it is strongly recommended

2 Agenda

- DDoS
- Guest lecture

3 Spoofed attacks

TCP reset attacks were so common against router BGP sessions for a period of time, and in response to this, the IETF suggested setting the TTL of BGP sessions to 254, as the overwhelming majority of legitimate sessions are within one hop, and the TTL field counts up.

4 DDoS

DDoS is an attack originating from a widely distributed network of clients. The motives for mounting such attacks used to be ego-based, and have become largely financial. MafiaBoy shut down many e-commerce sites with a SYN flood attack.

Circa 2003, there were more than 5000 attacks per week, of which 80% were vindictive "script kiddy" attacks. About 15% are more serious attacks, and the rest attacked the infrastructure directly (DNS servers, routes, etc). The current state of affairs is that there are many more attacks ongoing at any given moment, but they tend to target the infrastructure in new ways, but many of the old-style connections

4.1 Attack types

4.1.1 SYN flood

Send the victim many SYN packets, potentially with spoofed sources. Explained more in depth in previous lectures.

4.1.2 NAPTHA

Establish many connections with the victim, and then abandon them after getting a FIN packet. Exhausts active TCP connections on the server by leaving many in the FIN_WAIT_1 state.

4.1.3 Half open connections

Sends only the start of a request (e.g. GE[T] or POS[T]). This exhausts the application level resources, as they are tied up.

4.1.4 Client attacks

Ties up application resources by sending random but otherwise normal client traffic. To avoid caching and maximize damage, cache busters and search pages are favorite targets for this.

4.1.5 DNS attack

Target the DNS servers of a victim.

4.1.6 Reflector attacks

By sending requests to various public resources with a spoofed return address of the victim, the origin of attacks can be hidden. In some cases, the attack is amplified as the response can be much larger than the original request. Memcached is a particularly egregious amplifier, as it allows UDP traffic, was publicly open, and can send extremely large responses to tiny requests. NTP and DNS are two other popular amplifiers.

4.1.7 Smurf amplification

By pinging the broadcast address of an internal network with the victims' address spoofed as the source. This was open by default in the beginning.

4.1.8 Infrastructure Attacks

Target the routers themselves.

4.2 Riverhead Networks solution

Dr. Bremler-Barr co-founded Riverhead Networks in 2000 which was purchased by Cisco in 2004 for 39 million USD. They provided a DDoS mitigation service.

By installing a small detector box on premise, it would contact out of band the guard host which would steal the victim's flows upstream via BGP, filter and then return the cleaned flows to the victim. Filtering is a multi-stage process with antispoofing, statistical analysis, layer 7 analysis, traffic limiting, and traffic shaping among others. Because only the detection application sits with the client, guard box resources can be shared between customers.

4.3 SDN DDoS Mitigation

Lior Shafir published a paper at INFOCOM in 2017 on how to split the mitigation load across all the switches in a SDN.

5 Advanced DDoS attacks

A traditional DDoS attack will simply add more normal users to the server. However, a more sophisticated approach is to maximize the damage per additional user.

5.1 Hash Collision attack

Bro, a popular open source intrusion detection system used a hash table to detect port scanning. By choosing source ips that conformed to a certain pattern, researchers were able to show that Bro stopped scanning all incoming traffic.

Some analytical work was done that compared open vs closed hash tables and found that closed hashing created high probabilities of hitting a problematic entry in the hash table.

5.2 TCP retransmission

Exploiting the timeout and retransmission mechanism of TCP.

Low-Rate TCP-Targeted Denial of Service Attacks, A. Kuzmanovic and E. W. Knightly, Sigcomm 2003

5.3 Yo-Yo Attack

Published by Dr. Bremler-Barr's group in 2015. By attacking autoscaling groups with alternating attacks with high and low intensity, they were able to extend the effect of attacks well beyond the original period of the attack.

6 Guest lecture

6.1 Cloudshare

Guest lecture by Dr. Zvi Guterman, CEO of Cloudshare.

Cloudshare offers IaaS with some PaaS and SaaS aspects. One of their main solutions is IT labs and IT training on top of that.

It turned into a Q&A session. Not much to take notes on.

6.2 Actual lecture

Dr. Guterman's focus has always been on pragmatic system, and practical applications.

6.2.1 Space Time tradeoffs

For example, given a k bit symmetric cipher that works in $O(1)$ time and $O(1)$ memory, we want to examine different strategies for attacking this cipher.

A brute force approach is to simply try each different key in turn. This takes $O(2^k)$ time and $O(1)$ space. The other end of the spectrum is to precompute all pairs of keys and ciphertexts for a given plaintext. This takes $O(1)$ time to lookup the answer and $O(2^k)$ space.

In 1980, Martin Hellman published a paper that described a generic scheme for moving along the space/time tradeoff.

If someone wants, he is interested in advising a project in this field of tradeoffs. However, he only arrives in Israel every 6 weeks or so. If someone is interested, Dr. Bremler-Barr will introduce.

References

[1] Mark Crovella and Balachander Krishnamurthy. *Internet Measurement: Infrastructure, Traffic and Applications*. John Wiley & Sons, Inc., New York, NY, USA, 2006.

[2] James F. Kurose and Keith Ross. *Computer Networking: A Top-Down Approach Featuring the Internet*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2nd edition, 2002.

[3] George Varghese. *Network Algorithmics,: An Interdisciplinary Approach to Designing Fast Networked Devices (The Morgan Kaufmann Series in Networking)*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2004.