DDoS detection and mitigation using BGP

Author

Wissem Chouk <chouk@kth.se >

Organization and Supervisor

The student will be conducting his thesis between the company DGC and the university KTH.

Company DGC AB, Sveavägen 145, 113 46 Stockholm, Sweden
Company Supervisor Karl Röstlund, Product Manager Data-communication, <karl.rostlund@dgc.se>

Supervisor <suggested> Panagiotis Papadimitratos, Department of Networks and Systems Engineering, <papadim@kth.se>
Examiner <suggested> Panagiotis Papadimitratos, Department of Networks and Systems Engineering, <papadim@kth.se>

Keywords

Network, Security, DDoS attacks, BGP, Mitigation, Routing.

Background

During the last years, an increase in cyberattacks has been noticed. The scope of these attacks are getting wider and they are being more publicized on the mainstream media as they are threatening the daily life of the end consumer. The latest world cyberattack, the WannaCry ransomeware attack has paralyzed more than 200,000 computers across 150 countries for 4 days in May 2017 [1]. It has been labeled as the worst attack that has ever been launched. This attack has brought attention on the importance of security in IT.
Even if the WannaCry ransomeware attack has been very effective, it relies on the SMB (Server Message Block), a transport protocol over TCP. This breach is specific to to the Windows XP OS.
If no breach is discovered the most common and, yet effective attack is the DDoS (Distributed Denial of Service) attack. With the increase of connected devices (e.g. IoT) and the easy access to the DDoS-for-hire services [2], the DDoS attacks became more elaborate and common as their frequency has doubled between the first and the third quarter of 2017 [3]. Moreover, the attacks are constantly evolving, becoming harder to mitigate. The latest DDoS attack in Sweden took place in October 2017 targeting Sweden's Transport Administration (Trafikverket) causing delays in the trains schedule and a breakdown of the ticket booking app [4].

Organizations that have had DDoS protection projects on the back burner are now reprioritizing these projects as their customers are demanding more protection against such attacks. DGC, as a Swedish ISP, is willing to improve its protection and to provide a better service to its customers as well as to its internal infrastructure.

Problem

Many mitigation techniques have been developed but they are either very expensive or safely kept internally within the operators. A real time DDoS attacks detection and mitigation mechanism became a priority for all ISPs.
The main methods for detecting attacks are typically based on traffic flow data (i.e. Cisco Netflow) or mirrored ports from Internet routers. Flow collectors analyse traffic header information up to layer 4 and mirrored traffic can be analyzed up to layer 7, but is much more demanding in terms of performance of hardware running the analysis.
Mitigation can be done in many ways. The main methods used are blackhole routing, filtering and limiting traffic [5] in routers or in purpose built hardware (scrubbing device). Routers can typically filter and limit traffic up to layer 4 and scrubbing devices can do DPI (Deep Packet Inspection) and filter traffic up to layer 7. Blackhole routing [6] is typically a last resort to protect the network from collateral damage. Once used it is effectively making the attack successful, removing the target/service from the Internet. The thesis will be focused on investigating different techniques to perform an efficient attack detection and mitigation. The idea is to bring novelty to the field of research by analyzing different way of mitigation, combining different methods to propose a better solution with the use of BGP (Border Gateway Protocol).

Goals

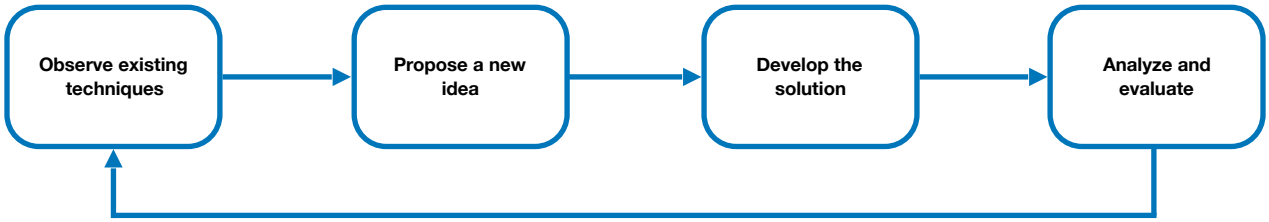
The expected outcome of this thesis is a deep analysis and evaluation of the existing solutions for DDoS detection and mitigation. A solution to mitigate the attacks is expected to be presented by the student. It should be based on standard protocols (i.e BGP). The company suggests the use of GoBGP, an open source BGP implementation based on the Go language.

Tasks

- Research the different methods used in DDoS detection and mitigation.
- Analyse the the methods by providing insights on different solutions and study the feasibility of each.
- Develop a tool to detect and mitigate DDoS attacks
- Test the solution in the labs of DGC

Method

The engineering method will be used for this thesis. The engineering method is based on the **observation of existing solutions** as mitigation techniques already exist but the purpose of the thesis is to bring a novelty to the existing techniques. Once the analysis done, the second phase is to **propose a new and better solution**. Then comes the **development stage**, where the application of the new solution should be made and transformed into a concrete tool. Afterwards, **analysis and evaluation** of the new proposal will be conducted in the labs of DGC. These 4 steps can be repeated for several times to improve the new solution.



References

[1] S. Mohurle, M.Patil , “A brief study of Wannacry Threat: Ransomware Attack 2017 “, International Journal of Advanced Research in Computer Science, Volume 8, No.5, May-June 2017, ISSN 0976-5697

[2] https://www.incapsula.com/ddos/booters-stressers-ddosers.html.

[3] Corero Network Security, Corero DDoS Trends Report, [Online] http://info.corero.com/rs/258-JCF-941/images/2017-q2q3-ddos-trends-report.pdf

[4] The Local Journal, 12 October 2017, [Online] https://www.thelocal.se/20171012/swedish-transport-agencies-targeted-in-cyber-attack.

[5] Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide, Release 5.2.x, [Online] https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r5-2/routing/configuration/guide/b_routing_cg52xasr9k/b_routing_cg52xasr9k_chapter_011.pdf

[6] W. Kumari, D. McPherson, “Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)”, August 2009, [Online] https://tools.ietf.org/html/rfc5635