Master Thesis on DDoS mitigation and detection

Karl Röstlund
DGC Access AB
Product manager Datacommunication
karl.rostlund@dgc.se

Background

DGC is a network operator and ISP primarily operating on the Swedish market for business and public organizations (no consumer services). Over time there has been an escalation in DDoS attacks, both in volume and frequency. As an operator, you have to deal with the increasing demand of protecting your customers and your infrastructure. The commercial tools for detecting and mitigating attacks in the ISP/Operator level has historically been very dominated by a few vendors. This has led to very expensive solutions and services.

For DGC DDoS-protection services has been offered as an added service to Internet access, but the production cost has been relatively high and therefore the kind of services are too expensive for many customers.

The main methods for detecting attacks are typically based on traffic flow data (i.e. Netflow) or mirrored ports from Internet routers. Flow collectors analyse traffic header information up to layer 4 and mirrored traffic can be analysed up to layer 7, but is obviously 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 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 and filter traffic up to layer 7. Blackhole routing is typically a last resort to protect your customer or network from collateral damage. Once used it is effectively making the attack successful, removing the target/service from the Internet. The most cost-effective way is often to use a combination of the other two measures; Using routers for rough filtering and scrubbing devices for more advanced filtering.

DGC have been looking at alternatives to the commercial products to increase flexibility and to drastically reducing cost of producing the services. A goal has been to provide a basic service as part of the Internet access services at no additional price. The service should be fully automated and handle some of the known and most frequent attack types (i.e. DNS and NTP amplification attacks).

Scope of the master Thesis

DGC wish that the student research and evaluate different technologies and solutions available in the field to detect and mitigate attacks. The solution should preferably be based on standard protocols and open source software. DGC suggests the use of GoBGP, an open source BGP implementation to investigate the different aspects of the network and the potential mitigation techniques. The student will have access to the lab, where any setup of the production networks can be reproduced/emulated. He will be able to run experiments and investigate solutions to mitigate DDoS attacks.

Some key technologies that DGC have identified are BGP flowspec and netflow. The expected outcome of the thesis would be a demo of a mitigation tool Based on the progression, the student could also include am a user interface for controlling mitigation as well as automating the mitigation action based on the detection of suspected attacks.