Automatically defend from DoS and DDoS traffic flood attacks
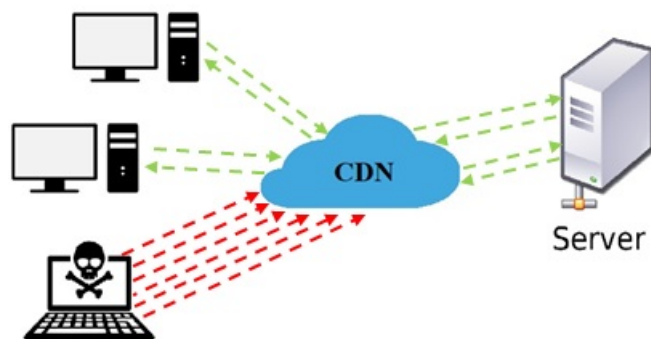
Yinon Cohen and Maor Shabtay

November 2017

DoS and DDoS attacks are attempts to exhaust server side assets, and designed to prevent client-to-server communication (denial of service). These attacks aim to both public and private sectors, and occur more and more frequently. In addition, lately the massive DDoS attacks are performing 100 Gigabits per second, and being more common than ever. These attacks are sowing fear among organizations and private server owners.

Our project deals with understanding and examining DoS and DDoS attacks, and what are the solutions for them. In particularly, we will discuss and handle with traffic flood attacks on web servers, and will try to develop our own software or algorithm to block or to give any immediately pragmatic solution.

Our main goal is to develop an automatic system that would identify and analyze a traffic flood attack, defend the server from it, and in need - will block any IP or sub-net which the flood comes from. Our system should run on a CDN instead of on the server in order to save the server's performances providing service

Advisor: Dr. Amit Dvir
Students:
Yinon Cohen 203526991
Maor Shabtay 305036162