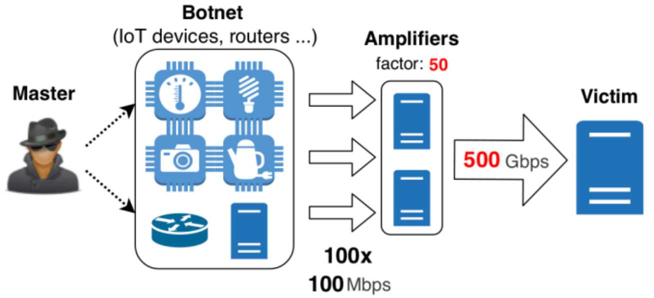
Informed DDoS Mitigation Based on Reputation

Author: Tomáš Jánský <janskto1@fit.cvut.cz>
Supervisor: Ing. Tomáš Čejka <cejkato2@fit.cvut.cz>

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

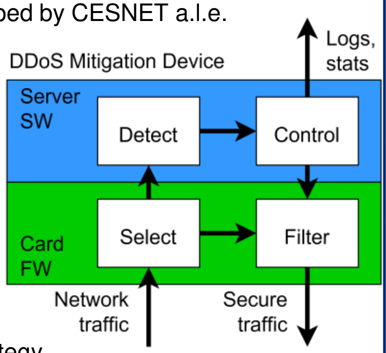
DDoS Amplification Attacks

- Attackers attempt to consume key resources of the victim.
- Malicious traffic is **amplified** by abusing legitimate servers.
- Amplified traffic is routed towards the victim thanks to the **spoofing** of the source IP address**.**

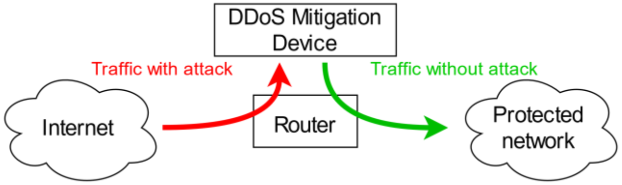


DDoS Mitigation Device (DMD)

- Scrubbing center developed by CESNET a.l.e.
- Commodity server equipped with an FPGA network interface card.
- Works at **100 Gb/s**.
- Discarding malicious packets.
- **Mitigation cycle**
  1. Capture traffic sample
  2. Analyze the sample
  3. Choose mitigation strategy
  4. Upload filtering rules back to FPGA

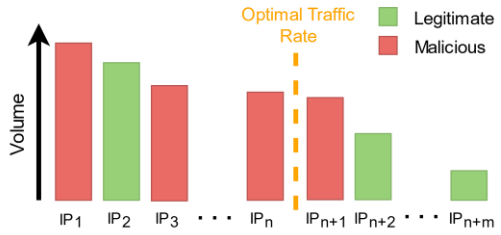


DMD Deployment



Problem: Preserving Legitimate Traffic

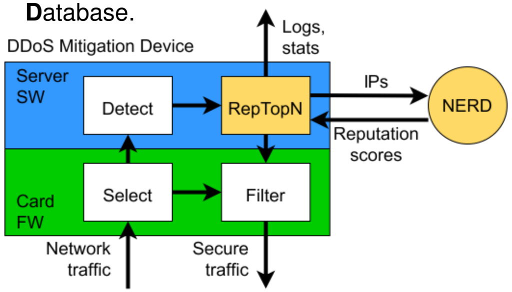
- **Defense strategy:** discarding traffic from **top-n** IP addresses which contribute the most to the overall traffic volume to reach optimal traffic rate.
- Fatal consequences in scenarios:
  1. Legitimate IP address produces more traffic than some attackers.



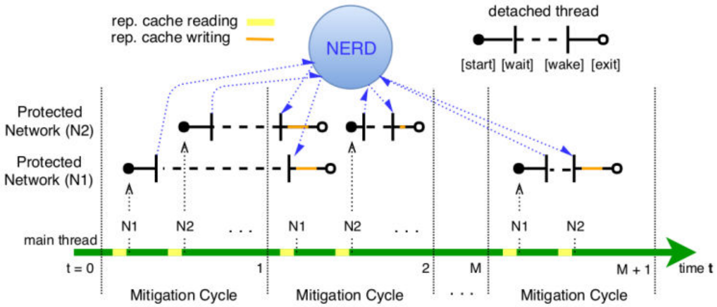
  2. A large number of attackers but every attacker produces only small amount of traffic.

Proposed Solution

- New mitigation heuristic **RepTopN**
  - ➢ Combines **volume contribution** and **reputation score** of IP addresses.
  - ➢ Based on **multiple-key sorting.**
- Reputation score
  - ➢ Number describing how likely the traffic originating from a certain IP address is malicious.
  - ➢ Assembled mainly from past behavior.
  - ➢ Obtained from **N**etwork **E**ntity **R**eputation **D**atabase.



Implementation and Testing



- Multithreaded communication with *NERD* ensures **negligible slowdown** of the mitigation cycle.
- Implemented reputation cache **significantly reduces** the frequency of queries to *NERD*.
- Identifying an attacker via reputation score leads to preserving legitimate traffic which would otherwise be disrupted.
- Successfully tested at **100 Gb/s** using a dedicated powerful hardware *Spirent Tester* device.
- Ready for other external sources of information to increase the probability of identifying attackers.

Contribution

- Improvement of real-time system for DDoS attacks mitigation.
- The **RepTopN** heuristic focuses on preserving connections of legitimate users during DDoS amplification attacks.
- Performs better than the previously used top-n in most cases.
- Online lookup of reputation score for observed IP addresses.
- Continuous reassembling of the list of IP addresses to discard.
- The developed system is deployed to defend *Czech National Research and Education Network* (NREN).
- The solution is undergoing the testing in real environment.

Publication: Jánský, T. et al.: Augmented DDoS Mitigation with Reputation Scores. In ARES *2018: International Conference on Availability, Reliability and Security, 2018, Germany.*

NERD: https://nerd.cesnet.cz

DMD: https://www.liberouter.org/technologies/ddos-protector/