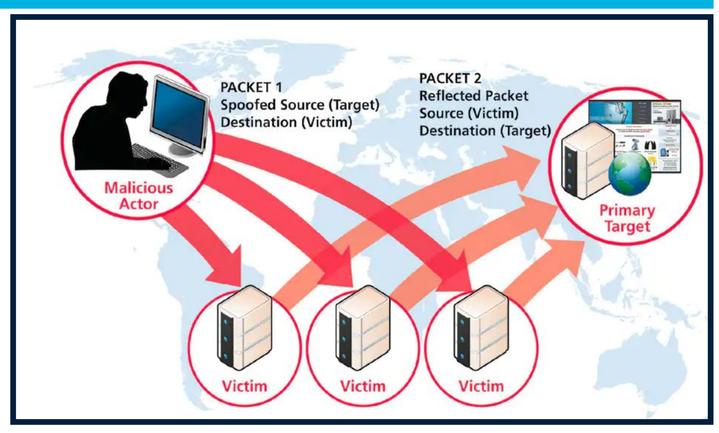
SDN-based System to Filter Out DRDoS Amplification Traffic in ISP Networks

Priyanka Dodia
Qatar Computing Research Institute, HBKU
Doha, Qatar
pgdodia@hbku.edu.qa

Yury Zhauniarovich
Perfect Equanimity
Minsk, Belarus
yury@perfectequanimity.com

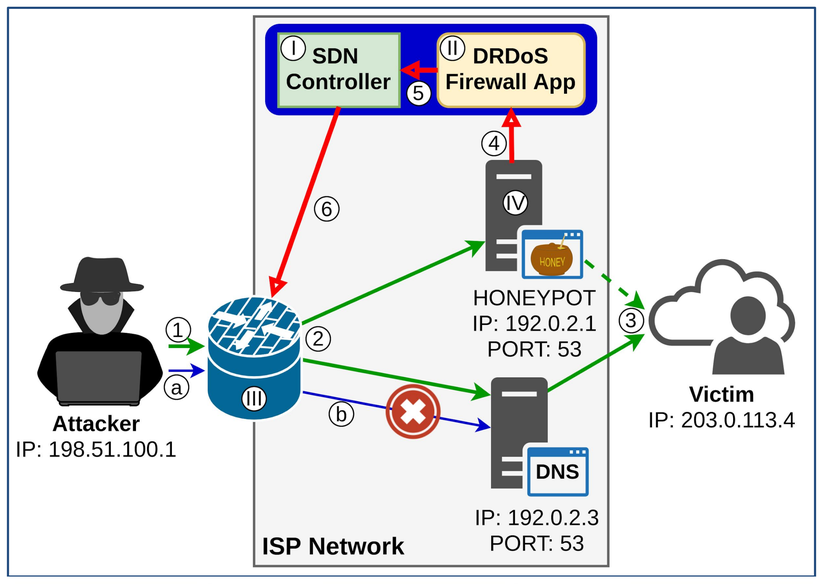
Motivation

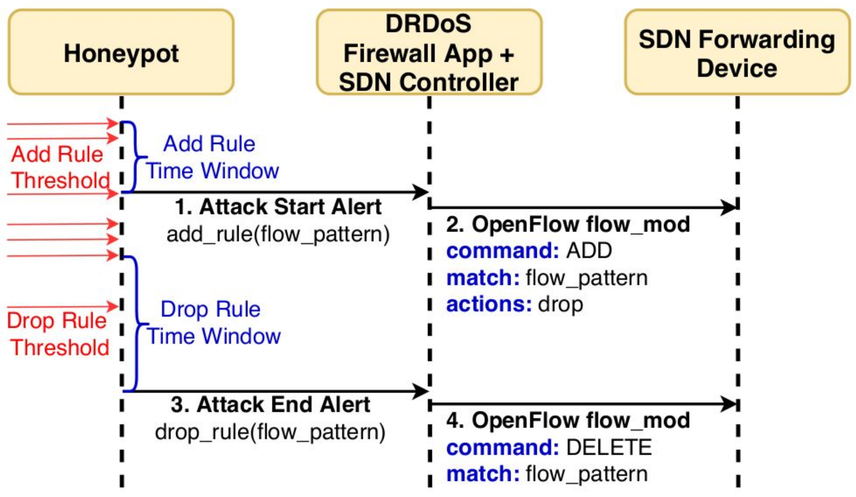
- ISPs suffer from Distributed Reflected Denial of Service (DRDoS) attacks.
- Attackers send spoofed requests to *amplifiers* which in turn reflect garbage traffic to victim SRC IP under target.
- ISPs host thousands of amplifiers, if abused, can collectively generate huge amounts of garbage data (~ 2TB per day) which may:
  - Exhaust ISPs' and their customers' bandwidth affecting Quality-Of-Service;
  - Degrade performance of client machines being abused for amplification;
  - Cause additional expenses for last mile ISPs as they buy bandwidth from upper tier providers



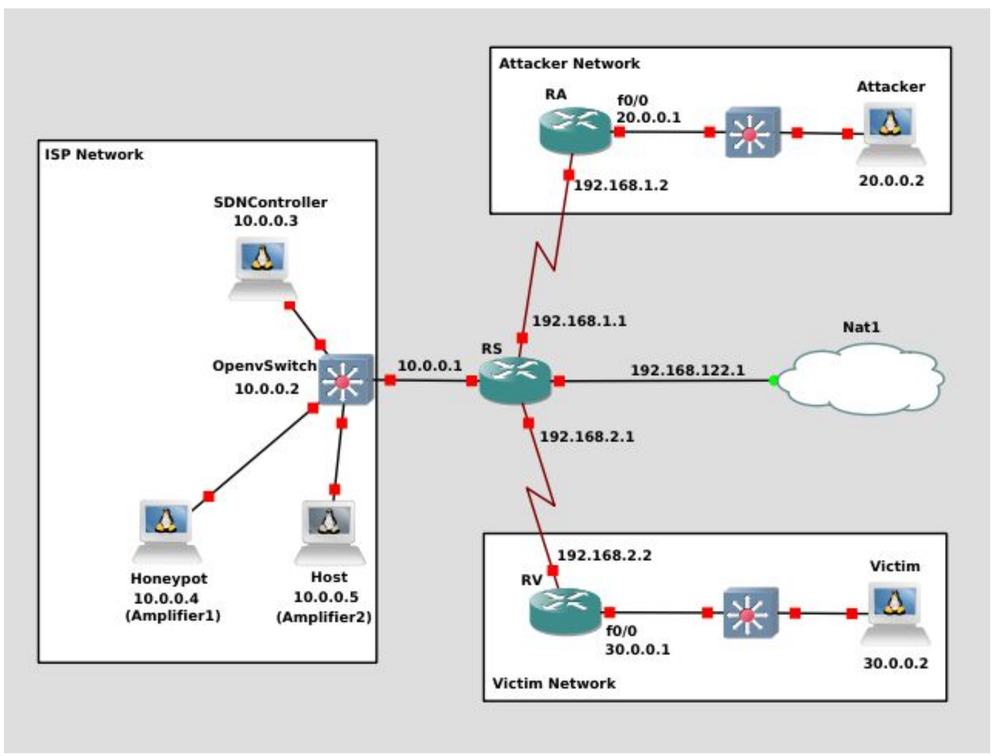
Solution

- A honeypot (*AmpPot* [1]) based system which detects spoofed requests in real time at ISP edge before they reach amplifiers within the ISP network.
- Unlike existing solutions, this work [2] aims at blocking DRDoS mid way before amplification phase, benefiting both ISPs implementing the system as well as victim(s) under attack by reducing the storm of amplified traffic.

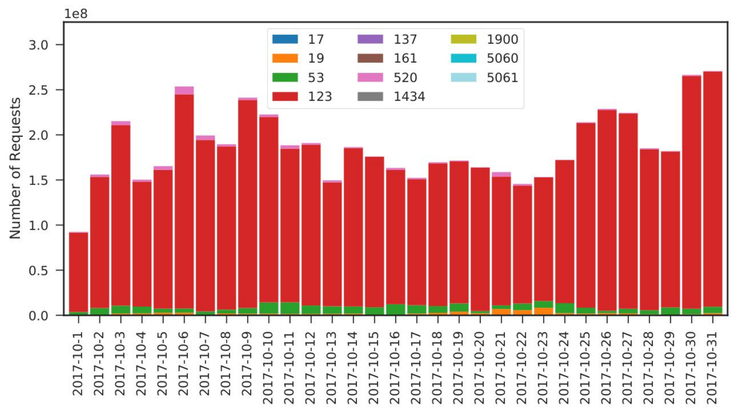




System Setup



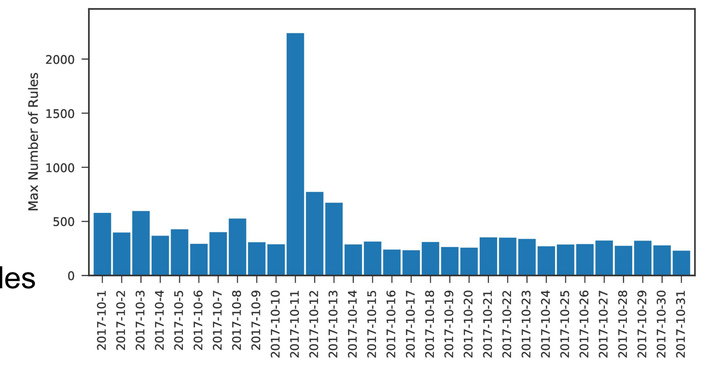
Feasibility Test On Real Attack Data

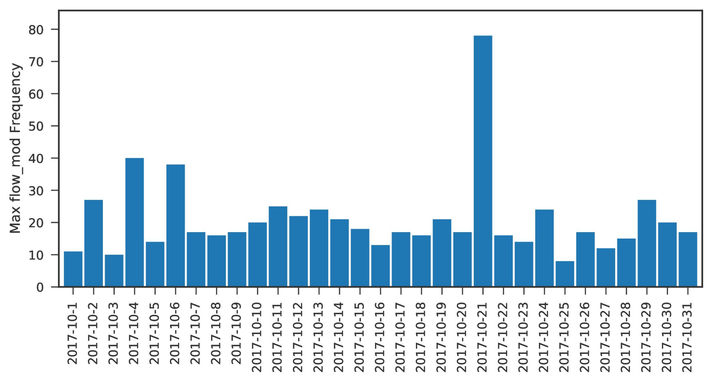


- Amt of attack requests received at honeypot each day
  - Test data: Oct 2017
  - 95 - 335 Million packets/day
  - NTP: 192.3 Million/day
  - UDP Port: 123

System Evaluation Parameters:

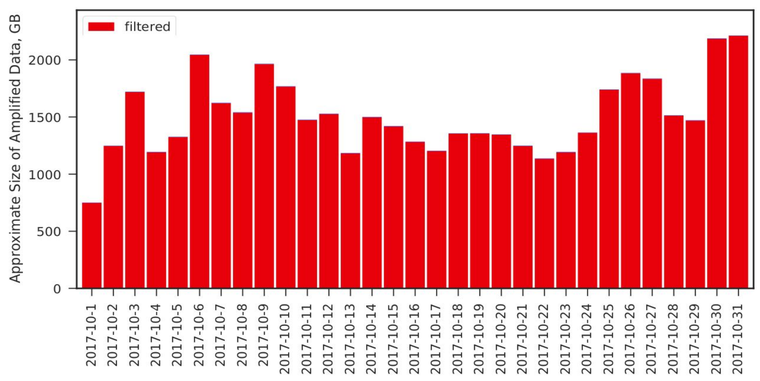
1. **Amt. of firewall rules generated* by DRDoS app during attacks (per second)**
   - Generic SDN switch table capaciy: ~ 8000-500,000 rules





2. **Frequency with which firewall rules generated* by DRDoS app (per second)**
   - Throughput of SDN Controllers: 38-1000 table modifications *(flow_mod/sec)*

- ***Approx* amount of garbage amplified traffic filtered out from ISP network (based on attack requests seen by honeypot)**
  - 750 GB - 2.2 TB per day



** feasibility test rules generated based on unique (Victim SRC IP, DST PORT) under attack*

Future Work

- Prevent honeypot detection and abuse:
  - Improve mimicking of vulnerable services
  - Use collective data from multiple honeypots installations
- Victim network blocking and collateral damage:
  - Throttling traffic rather than complete blocking of UDP service for victim
  - Filtering with deep packet inspection (eg: monlist abused in NTP)

References:
1. L. Krämer, J. Krupp, D. Makita, T. Nishizoe, T. Koide, k. Yoshioka, and C. Rossow, "AmpPot: Monitoring and Defending Against Amplification DDoS Attacks," in Proc. of RAID, 2015, pp. 615–636.
2. Y. Zhauniarovich and P. Dodia. "Sorting the Garbage: Filtering Out DRDoS Amplification Traffic in ISP Networks," In Proc. of IEEE NetSoft, 2019, pp. 142-150