Signature-based Traffic Classification and Mitigation for DDoS Attacks using Programmable Network Data Planes

Marinos Dimolianis, Adam Pavlidis, Vasilis Maglaris
Network Management & Optimal Design Laboratory (NETMODE)
School of Electrical & Computer Engineering
National Technical University of Athens

P4 and Data Plane Programming BoF
June 18th, 2021
Virtual Meeting

DDoS Attack Detection & Mitigation

- Traditional Approaches
  - Source IP/Flow-based
    - Metrics Collection, Storage & Analysis -> Delayed Detection
    - Massive number of sources -> Filtering scalability
  - Static signatures
    - Inability to adapt in unseen attack patterns
- Dynamic Signature-based Classification & Filtering
  - High-Performance Programmable Data Planes
    - Monitoring & Filtering
  - Supervised Machine Learning for Traffic Classification

Signature-based Classification & Filtering

- Fine-grained packet monitoring powered by XDP
  - Packet fields collection ranging from Network to Application Layer (Signatures)
- Signature Classification via Supervised Learning
  - Random Forests, Multilayer Perceptrons
- Signature Reduction
  - Pinpoint the fields that describe optimally the attack traffic
- Traffic filtering using programmable firewalls (XDP) based on salient attacks characteristics

Use Case: DNS Amplification Attacks

- Accurate DNS Traffic Classification on real traffic
  - True Positive Rate ~ 99%, True Negative Rate ~ 98%
- Signature-based schemes require less monitoring data than IP-based to filter more attack traffic
- #Malicious DNS Signatures << #Malicious IP sources
- Efficient Traffic Monitoring and Filtering (XDP)
  - Single-CPU monitors/filters up to 5Mpps
  - Horizontal & Vertical Scaling

Future Directions

- Signature Exchange Mechanisms in Federated Environments (e.g. NRENs)
  - Privacy-Preserving Traffic Classification – Federated Learning
- Collaborative Filtering – Upstream DDoS Blocking
  - Offered as-a-Service leveraging programmable data planes scalability
- Signature-based Filtering at Programmable Network Devices (e.g. P4-enabled Routers)
  - BGP *FlowSpec* Payload Matching[1]

1. https://datatracker.ietf.org/doc/draft-khare-idr-bgp-flowspec-payload-match/

Marinos Dimolianis
mdimolianis@netmode.ntua.gr

THANK YOU!