Volumetric DRDoS attacks can completely overwhelm a victim network. How can we filter out DRDoS attack traffic upstream, so that the target AS’s bandwidth is not exhausted?

- Build a DRDoS defense specifically designed to be deployed at IXPs
- Filter DRDoS traffic at IXPs where the victim (or its upstream providers) peers with other networks

**Approach**

NetFlow-based DRDoS detection system:
- Consume NetFlow stats from IXP network
- Time series analysis using EWMA
- Keep track of traffic volume trends per each (srcPort, dstAS) pair
- Raise DRDoS attack alert if anomaly is found for a (srcPort, dstAS) pair and traffic is “evenly” distributed across multiple source ASes

**Preliminary Results**

Examples of interesting in-the-wild DRDoS attacks

**Ongoing Work**

- Ongoing deployment at SoX
- Longitudinal analysis of DRDoS attacks
- Correlation with BGP data to infer whether any attack mitigation was deployed
- Data collection and analysis at other IXPs

This material is based upon work supported by the National Science Foundation with Grant No. 1741608.

Contacts: ks54471@uga.edu, perdisci@cs.uga.edu, mkonte@gatech.edu