Cloud-scale Attacks

Cloud services become an attractive target of attacks
- **Large-scale**: 100s of Gbps
- **Diverse types**: network-layer & application layer
- **Fast ramp-up rate**: within a few minutes

Existing approaches
- Commercial hardware boxes (e.g. Firewall, IDS, DDoS-protection appliance)
  - **Low Capacity**: cannot accommodate attack volume
  - **High Cost**: unfavorable cost vs. capacity tradeoffs
  - **Inflexible**: lack of programmability
- Commercial attack prevention services (e.g. CloudFlare, Prolexic)
  - Risk of privacy and confidential leakage

NIMBUS Design

1. **Flexible sampling**
   - Key idea
     - According to traffic statistics estimated from traffic samples
     - Iteratively adjust sample rates for different flows
   - Challenges
     - Allocate sampling resources for better detection accuracy

2. **Auto-scale**
   - Key idea
     - VMs may be overloaded under attack scenario
     - Controller migrates some of flows to other or new VMs
   - Challenges
     - Which flows and associated states to migrate
     - Balance the detection responsiveness and consistency

3. **Detection and Mitigation**
   - Key idea
     - Flexible for diverse and new attack detection support
     - Generic to support existing detection tools (e.g. DPI)
   - Challenges
     - Robust to wise adversaries who know NIMBUS system
     - (e.g. short-lived attack, low-rate attack, etc.)

Attack-Detection-as-a-Service

Challenges
- **Auto-scale** to match traffic capacity and enable agility
- **Programmability** to handle new and diverse types of attacks
- **Fast and accurate** detection and mitigation
- **Robustness** to wise adversaries

Solution

**NIMBUS** for cloud-scale attack detection and mitigation
1) Elasticity of cloud computing resources
2) Programmability in software-defined networks (SDN)

Prototype and Preliminary Results

**Prototype**
- Implemented Heavyhitter detection in VMs
- VMs report detection results and its load to controller
- Controller updates traffic routing to balances the load across VMs
- Controller instantiates new VMs to accommodate traffic capacity

**Preliminary Results**
- We add 9 Gbps attack burst from 15th second
- The detection accuracy decreases during auto-scale
- As more VMs instantiated, the detection accuracy recovers
- System scaling to accommodate attack volume