Inter-domain cooperative DDoS protection problems and mechanism

draft-nishizuka-dots-inter-domain-mechanism-00

Kaname Nishizuka  NTT Communications
Liang Xia  Huawei
Jinwei Xia  Huawei
DaCheng Zhang  Alibaba
Luyuan Fang  Microsoft

April 2016  Buenos Ayres
Overview

Cooperative DDoS Protection:
• utilize other organization's resources each other through DOTS to share the burden of the protection

This draft describes:
1. Architecture & Problems
2. Protocol
of the “Cooperative DDoS Protection”
Architecture of Cooperative DDoS Protection

• 2 or more DDoS protection service providers are cooperating with each other via DOTS
• Focusing on the relationship of those providers

Distributed Architecture

Centralized Architecture

SP: DDoS Protection Service Provider
Peer-to-peer coordination:
- customer<->DOTS client, ISP controller<->DOTS server + DOTS client;
- The inter-domain coordination can be a repeated process;
- A straightforward and simple solution for the DDoS protection cooperation among small number of ISPs:
  - The incomplete information may not lead to the most optimized operation;
  - Configurations become more complex and error prone as the number of ISPs increases;
  - By repeated coordination among multiple ISPs, it may take a long time to enforce the mitigation.
Centralized Architecture

- The centralized orchestrator is the core component to the inter-domain system;
- Customer<->DOTS client, ISP controller<->DOTS server + DOTS client, orchestrator<->DOTS server + DOTS client;
- The inter-domain coordination is bridged by the orchestrator;
- Comparing to distributed architecture:
  - The orchestrator has the HA problem;
  - Centralized way facilitates the automatic provisioning of DDoS protection resource and comprehensive information for overall optimized mitigation;
  - Direct communication with orchestrator guarantees quick and fixed DDoS response time.
Challenges for Inter-domain Cooperative DDoS Protection

1. Bootstrapping Problems (automatic provisioning):
   – Trust relation and secure channel set up;
   – Auto-discovery and capability negotiation, etc.

2. Coordination problems:
   – How to get the appropriate mitigation service from other operators with high efficiency: make the decision based on information sharing;
   – Near source mitigation: spoofed address, privacy protection;
   – Others: accounting, returning path, etc.