Adding DDoS Types for DOTS signaling

Yang Bo

2018.7

Agenda

- **What** is DoS type definition
- **Why** DoS type is needed in DOTS signaling
- **How** to include DoS type in DOTS signaling protocol

Background

- DoS attacks can be formed in different ways. Different mechanism requires different mitigation method
  - Network layer: ICMP
  - Transport layer: TCP， UDP
  - Application layer: HTTP, SIP, DNS, NTP, …
- Different vendors have different view point on classifying DoS, which leads to interworking issues

A sample framework of DoS Types

It is hard to define a full table of DoS type, but it is possible to have an extendable framework in the current stage. Here is an example that we apply in our network.

Layer	Protocols	Attack Types	Attack Sub-type
Network	ICMP	ICMP Flood	
		ICMP Fragment	
Transport	UDP	UDP Flood	
		UDP Fragment	
	TCP	ACK Flood	
		SYN Flood	
		FIN/RST Flood	
		TCP Misuse	
		TCP Connection Flood	
		TCP Fragment	
Application	HTTP	HTTP Flood	HTTP Get/Post Flood HTTP CC Attack
		HTTP Slow Attack	Slow POST Slow Headers
	HTTPS	HTTPS Flood	
	SIP	SIP Flood	
	DNS	DNS Query Flood	
		DNS Reply Flood	
		DNS Amplification	
	SSDP	SSDP Amplification	
	NTP	NTP Amplification	
	Chargen	Chargen Amplification	
	SNMP	SNMP Amplification	
	Extended	<Protocol + Port>	<user-defined type string>

Agenda

- **What** is DoS type definition
- **Why** DoS type is needed in DOTS signaling
- **How** to include DoS type in DOTS signaling protocol

Benefit of DoS type for DOTS

- For the DOTS client
  - It is easier to get DoS type from attack target
  - It helps to make decision on which server to send the DOTS mitigation requests, in the 1C:nS connection topology
- For the DOTS gateway
  - It helps to aggregate the same type of attacks, for a more efficiency communication, if needed
  - It helps the DOTS gateway to have the information about the network status, and helps to analysis and statistics
- For the DOTS server
  - It helps to orchestrate these mitigators on demand
  - With the information the attack target provided as reference, the mitigator shall be able to take action quickly, without parse the attack traffic in details.

- With the DoS type included in DOTS signaling, shared information between client, gateway and server, each node shall have more information about the DoS attack. new business model can be setup based on this.

Agenda

- **What** is DoS type definition
- **Why** DoS type is needed in DOTS signaling
- **How** to include DoS type in DOTS signaling protocol

Include DoS type in DOTS signal

- “DoS-Type”（string), as an optional field, can be added into the data model of each mitigation methods as follows:

```
{
  "target-prefix": [
    "string"
  ],
  ......
  "target-uri": [
    "string"
  ],
  "DoS-type": [
    "string"
  ],
  "alias-name": [
    "string"
  ],
  "lifetime": integer
}
```

A “DoS-type” definition text as well as the table can be provided as the reference

Way forward

- If time allows, we can discuss and refine the current DoS-type before it is included into the draft
- If no, we wish it can be included in future work

Thanks!