Introduce DoS type for DOTS signaling
draft-yang-dos-type-for-dots-00

Abstract

The purpose of this document is to analyze the usage of DoS type in DOTS signaling, provide a classification framework for DoS type, and give suggestions on introducing DoS-Type into DOTS signaling.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 2, 2019.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
1. Introduction

DOTS defines a method of coordinating defensive measures among willing peers to mitigate attacks quickly and efficiently, DOTS signaling enables hybrid attack coordination between DOTS client that talks with attack target and DOTS server that talks with Mitigators [draft-ietf-dots-architecture]. But in [draft-ietf-dots-signal-channel] the YANG module "ietf-dots-signal-channel" did not include the DoS-Type field, which is important for the DDoS mitigation as well as network operations.

DoS attacks can be generated using different mechanisms, such as ICMP Flood, TCP Flag Misuse, DNS replay. Here list some DoS that occurs in different layer:

- Network layer: ICMP
- Transport layer: TCP, UDP
- Application layer: HTTP, SIP, DNS, NTP, ...

Different DDoS mechanisms may require different mitigation methods, but currently, different vendors have different viewpoints on classifying DoS, which leads to interoperating and interworking issues.

This document is to analyze the usage of DoS type in DOTS signaling, provide a classification framework for DoS type, and give suggestions on introducing DoS-Type into DOTS signaling.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].
3. Terminology and Abbreviations

The terminology and abbreviations used in this document are defined in this section.

- **DDoS**: A distributed denial-of-service attack, in which traffic originating from multiple sources is directed at a target on a network. DDoS attacks are intended to cause a negative impact on the availability and/or other functionality of an attack target. Denial-of-service considerations are discussed in detail in [RFC 4732].

- **DDoS attack target**: A network connected entity with a finite set of resources, such as network bandwidth, memory or CPU, that is the target of a DDoS attack. Potential targets include (but are not limited to) network elements, network links, servers, and services.

- **Mitigator**: An entity, typically a network element, capable of performing mitigation of a detected or reported DDoS attack. The means by which this entity performs these mitigations and how they are requested of it are out of scope. The mitigator and DOTS server receiving a mitigation request are assumed to belong to the same administrative entity.

4. Usage of DoS-type in DOTS signaling

Various DoS-type means different attack method, may need different mitigation method also. If DoS-type is included in to the DOTS signalling message, it will helps:

- **Message routing**:

  - DOTS Client: shall be able to make decision on which server to send the DOTS mitigation requests, in the one-Client multiple Server connection topology, according to predefined server capability configurations.

  - DOTS Server: considering there are different kind of mitigators, each kind provides some types of DoS mitigation service accrodingly, the DOTS server shall need to know which mitigator is suitable for ceritain DoS attack. This is very common situation when the mitigator is deployed in a virtualized resource pool.

Analysis and Statistics:
Both the DOTS gateway and DOTS server shall need to analysis and/or statistic the amount DoS attack and mitigation informations for operational purpose.

5. Definition of DoS-type

As we mentioned different vendors have different viewpoint on classifying DoS, New DoS types are constantly emerging, we can not can’t enumerat all the DOS types exhaustively. But we can define an open framework, that includes all common DoS types, while allows easy extension.

The DoS type framework is classified into different layers, i.e., Network Layer, Transport Layer, Application Layer. Listed as follows:
<table>
<thead>
<tr>
<th>Layer</th>
<th>Protocols</th>
<th>Attack-Type</th>
<th>Attack-Subtype</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>ICMP</td>
<td>ICMP-Flood</td>
<td>ICMP-Fragment</td>
</tr>
<tr>
<td>Transport</td>
<td>UDP</td>
<td>UDP-Flood</td>
<td>UDP-Fragment</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>ACK-Flood</td>
<td>SYN-Flood</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FIN_RST-Flood</td>
<td>TCP-Flag-Misuse</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP-Connection-Flood</td>
<td>TCP-Connection-Flood</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP-Fragment</td>
<td>TCP-Fragment</td>
</tr>
<tr>
<td>Application</td>
<td>HTTP</td>
<td>HTTP-Flood</td>
<td>Get_Post-Flood</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HTTP-Slow-Attack</td>
<td>CC-Attack</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Slow-POST</td>
<td>Slow-Headers</td>
</tr>
<tr>
<td></td>
<td>HTTPS</td>
<td>HTTPS-Flood</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SIP</td>
<td>SIP-Flood</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS</td>
<td>DNS-Query-Flood</td>
<td>DNS-Reply-Flood</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DNS-Amplification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSDP</td>
<td>SSDP-Amplification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NTP</td>
<td>NTP-Amplification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chargen</td>
<td>Chargen-Amplification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNMP</td>
<td>SNMP-Amplification</td>
<td></td>
</tr>
<tr>
<td>Extended</td>
<td>‘string’</td>
<td>‘user-defined-type-string’</td>
<td></td>
</tr>
</tbody>
</table>

Table 1. DoS-Type definition framework.

According to Table 1:

- This framework shall allow service providers, vendors to define their extended DoS type.
- The representation of each DoS type shall use a string type, and take the form of "Attack-type.Attack-Subtype".
6. Suggestion on adding DoS-type into DOTS signaling message

According to the [draft-ietf-dots-signal-channel] the YANG module "ietf-dots-signal-channel" a DoS-Type field shall be added as follows:

---rw (message-type)?
  +=-(mitigation-scope)
    +=-rw scope* [cuid mid]
      +=-rw cdid?             string
      +=-rw cuid              string
      +=-rw mid               uint32
      +=-rw target-prefix*    inet:ip-prefix
      +=-rw target-port-range* [lower-port upper-port]
       | +=-rw lower-port      inet:port-number
       | +=-rw upper-port       inet:port-number
      +=-rw target-protocol*  uint8
      +=-rw target-fqdn*      inet:domain-name
      +=-rw target-uri*       inet:uri
      +=-rw DoS-Type*          string
      +=-rw alias-name*        string
      +=-...

Figure 2

7. Normative References


Author’s Address

Yang Boyle
China Mobile
China

Email: boyxd@hotmail.com