Abstract

This document specifies an extension to the DOTS signal channel to control the filtering rules during attack mitigation.

This extension allows a DOTS client to activate or de-activate filtering rules during a DDoS attack. The characterization of these filters is supposed to be conveyed by a DOTS client during peace time by means of DOTS data channel.

Editorial Note (To be removed by RFC Editor)

Please update these statements within the document with the RFC number to be assigned to this document:

- "This version of this YANG module is part of RFC XXXX;"
- "RFC XXXX: Controlling Filtering Rules Using DOTS Signal Channel;"
- reference: RFC XXXX
- [RFCXXXX]

Please update these statements with the RFC number to be assigned to the following documents:

- "RFC SSSS: Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Specification" (used to be [I-D.ietf-dots-signal-channel])
- "RFC DDDD: Distributed Denial-of-Service Open Threat Signaling (DOTS) Data Channel Specification" (used to be [I-D.ietf-dots-data-channel])
Please update the "revision" date of the YANG module.

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 http://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 May 25, 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 (http://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.

Table of Contents

1. Introduction .................................................... 3
  1.1. The Problem ............................................. 3
  1.2. The Solution ............................................ 4
2. Notational Conventions and Terminology ........................ 4
3. Controlling Filtering Rules ..................................... 4
  3.1. Binding of the Data Channel and Signal Channel ............ 4
  3.2. DOTS Signal Channel Extension ............................ 5
    3.2.1. Filtering Control .................................. 5
    3.2.2. DOTS Signal Filtering Control Module ................. 6
      3.2.2.1. Tree Structure ................................. 6
      3.2.2.2. YANG Module .................................... 6
4. IANA Considerations ............................................ 9
1. Introduction

1.1. The Problem

The DOTS data channel protocol [I-D.ietf-dots-data-channel] is used for bulk data exchange between DOTS agents to improve the coordination of all the parties involved in the response to the DDoS attack. Filter management is one of its tasks which enables a DOTS client to retrieve DOTS server filtering capabilities and to manage filtering rules. Filtering rules are used for dropping or rate-limiting unwanted traffic, and permitting accept-listed traffic.

Unlike the signal channel, the data channel is not expected to deal with attack conditions. As such, an issue that might be encountered in some deployments is when filters installed by means of DOTS data channel protocol may not function as expected during DDoS attacks or exacerbate an ongoing DDoS attack. The DOTS data channel cannot be used then to change these filters, which may complicate DDoS mitigation operations.

A typical case is a DOTS client which configures during peace time filtering rules using data channel to permit traffic from accept-listed sources, but during the volumetric DDoS attack the DDoS mitigator identifies the source addresses/prefixes in the accept-listed filtering rules are attacking the target. For example, an attacker can spoof the IP addresses of accept-listed sources to generate attack traffic or the attacker can compromise the accept-listed sources and program them to launch DDoS attack.

[I-D.ietf-dots-signal-channel] is designed so that the DDoS server notifies the conflict to the DOTS client (‘conflict-cause’ set to 2 (Conflicts with an existing accept list)), but the DOTS client may not be able to withdraw the accept-listed filtering rules during the attack period due to the high-volume attack traffic saturating the inbound link. In other words, the DOTS client cannot use the DOTS data channel to withdraw the accept-listed filters when the DDoS attack is in progress. This assumes that this DOTS client is the owner of the filtering rule.
1.2. The Solution

This specification addresses the problems discussed in Section 1.1 by adding the capability of managing filtering rules using the DOTS signal channel, which enables a DOTS client to request the activation or de-activation of filtering rules during a DDoS attack.

The DOTS signal channel protocol [I-D.ietf-dots-signal-channel] is designed to enable a DOTS client to contact a DOTS server for help even under severe network congestion conditions. Therefore, extending the DOTS signal channel protocol to manage the filtering rules during an attack will enhance the protection capability offered by DOTS protocols.

Note: The experiment at the IETF103 hackathon showed that even when the incoming link is saturated by DDoS attack traffic, the DOTS client can signal mitigation requests using the DOTS signal channel over the saturated link.

Conflicts that are induced by filters installed by other DOTS clients of the same domain are not discussed in this specification.

2. Notational Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", " SHALL", " SHALL NOT", 
"SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and 
"OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The reader should be familiar with the terms defined in [I-D.ietf-dots-requirements].

3. Controlling Filtering Rules

3.1. Binding of the Data Channel and Signal Channel

The filtering rules eventually managed using the DOTS signal channel must be created a priori by the same DOTS client using the DOTS data channel. Managing conflicts with filters installed by other DOTS clients of the same domain is out of scope.

As discussed in Section 4.4.1 of [I-D.ietf-dots-signal-channel], a DOTS client must use the same ‘cuid’ for both the signal and data channels. This requirement is meant to facilitate binding channels used by the same DOTS client.
The DOTS signal and data channels from a DOTS client may or may not use the same DOTS server. Nevertheless, the scope of the mitigation request, alias, and filtering rules are not restricted to the DOTS server but to the DOTS server administrative domain. To that aim, DOTS servers within a domain are assumed to have a mechanism to coordinate the mitigation requests, aliases, and filtering rules to coordinate their decisions for better mitigation operation efficiency. The exact details about such mechanism is out of scope of this document.

A filtering rule controlled by the DOTS signal channel is identified by its Access Control List (ACL) name. Note that an ACL name unambiguously identifies an ACL bound to a DOTS client, but the same name may be used by distinct DOTS clients.

The activation or de-activation of an ACL by the signal channel overrides the ‘activation-type’ (defined in Section 7.2 [I-D.ietf-dots-data-channel]) a priori conveyed with the filtering rules using the DOTS data channel.

3.2. DOTS Signal Channel Extension

3.2.1. Filtering Control

This specification extends the mitigation request defined in [I-D.ietf-dots-signal-channel] to convey the intended control of the configured filtering rules. The DOTS client conveys the following parameters in the CBOR body of the mitigation request:

acl-name: A name of an access list defined in the data channel.

As a reminder, an ACL is an ordered list of Access Control Entries (ACE). Each Access Control Entry has a list of match criteria and a list of actions. The list of configured ACLs can be retrieved using the DOTS data channel during peace time.

This is an optional attribute.

activation-type: Indicates the activation type of an ACL overriding the existing ‘activation-type’ installed by the DOTS data channel. This attribute can be set to ‘deactivate’, ‘immediate’, or ‘activate-when-mitigating’ defined [I-D.ietf-dots-data-channel]. Note that ‘immediate’ or ‘activate-when-mitigating’ are equivalent when a mitigation request is being processed by the server.

If this attribute is not provided, the DOTS server MUST use ‘activate-when-mitigating’ as the default value.
This is an optional attribute.

If the DOTS server does not find the ACL name conveyed in the mitigation request in its configuration data for this DOTS client, it MUST respond with a "4.04 (Not Found)" error response code.

3.2.2. DOTS Signal Filtering Control Module

3.2.2.1. Tree Structure

This document augments the "dots-signal-channel" DOTS signal YANG module defined in [I-D.ietf-dots-signal-channel] for managing the filtering rules.

This document defines the YANG module "ietf-dots-signal-control-filter", which has the following tree structure:

module: ietf-dots-signal-control-filter
 augment /ietf-signal:dots-signal/ietf-signal:message-type
 /ietf-signal:mitigation-scope/ietf-signal:scope:
  +--rw acl-list* [acl-name] {control-filtering}?
     +--rw acl-name
          |   -> /ietf-data:dots-data/dots-client/acls/acl/name
     +--rw activation-type? enumeration

3.2.2.2. YANG Module

<CODE BEGINS> file "ietf-dots-signal-control-filter@2018-11-20.yang"

module ietf-dots-signal-control-filter {
  yang-version 1.1;
  namespace
  prefix signal-control-filter;

  import ietf-dots-signal-channel {
    prefix ietf-signal;
    reference
      "RFC SSSS: Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Specification";
  }

  import ietf-dots-data-channel {
    prefix ietf-data;
    reference
      "RFC DDDD: Distributed Denial-of-Service Open Threat Signaling (DOTS) Data Channel Specification";
  }

<CODE ENDS>
This module contains YANG definition for the signaling messages exchanged between a DOTS client and a DOTS server for the DOTS signal channel controlling the filtering rules configured using the DOTS data channel.

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

Redistribution and use in source and binary forms, with or without modification, is permitted pursuant to, and subject to the license terms contained in, the Simplified BSD License set forth in Section 4.c of the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info).

This version of this YANG module is part of RFC XXXX; see the RFC itself for full legal notices.

revision 2018-11-20 {
  description
    "Initial revision.";
  reference
    "RFC XXXX: Controlling Filtering Rules Using DOTS Signal Channel ";
}

feature control-filtering {
  description
    "This feature means that DOTS signal channel is able to
manage the filtering rules created by the same DOTS client using the DOTS data channel.
}


description "ACL name and activation type";

list acl-list {
  key "acl-name";
  description "List of ACLs as defined in the DOTS data channel. These ACLs are uniquely defined by cuid and name.";
  leaf acl-name {
    type leafref {
      path "/ietf-data:dots-data/ietf-data:dots-client/" + "ietf-data:acls/ietf-data:acl/ietf-data:name";
    }
    description "Reference to the ACL name bound to a DOTS client.";
  }
  leaf activation-type {
    type enumeration {
      enum "activate-when-mitigating" { value 1;
        description "The ACL is installed only when a mitigation is active. The ACL is specific to this DOTS client.";
      }
      enum "immediate" { value 2;
        description "The ACL is immediately activated.";
      }
      enum "deactivate" { value 3;
        description "The ACL is maintained by the server, but it is deactivated.";
      }
    }
    description "Set the activation type of an ACL.";
  }
}
4. IANA Considerations

4.1. DOTS Signal Channel CBOR Mappings Registry

This specification registers the 'activation-type' parameter in the IANA "DOTS Signal Channel CBOR Mappings" registry established by [I-D.ietf-dots-signal-channel].

The 'activation-type' is a comprehension-required parameter. The 'acl-list' and 'acl-name' parameters are defined as comprehension-required parameters in Table 6 in [I-D.ietf-dots-signal-channel]. Following the rules in [I-D.ietf-dots-signal-channel], if the DOTS server does not understand the 'acl-list' or 'acl-name' or 'activation-type' attributes, it responds with a "4.00 (Bad Request)" error response code.

Note to the RFC Editor: Please delete (TBD1) once the CBOR key is assigned from the 0x8000 - 0xBFFF range.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>YANG Type</th>
<th>CBOR Key</th>
<th>CBOR Major Type &amp; Information</th>
<th>JSON Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>activation-type</td>
<td>enumeration</td>
<td>0x0031</td>
<td>0 unsigned (TBD1)</td>
<td>String</td>
</tr>
</tbody>
</table>

4.2. DOTS Signal Control Filtering YANG Module

This document requests IANA to register the following URI in the "IETF XML Registry" [RFC3688]:

```
Registrant Contact: The IESG.
XML: N/A; the requested URI is an XML namespace.
```

This document requests IANA to register the following YANG module in the "YANG Module Names" registry [RFC7950].
5. Security Considerations

The security considerations discussed in [I-D.ietf-dots-signal-channel] and [I-D.ietf-dots-data-channel] need to be taken into account.

6. Acknowledgements

TBD

7. References

7.1. Normative References

[I-D.ietf-dots-data-channel]

[I-D.ietf-dots-signal-channel]


7.2. Informative References

[I-D.ietf-dots-requirements]
Mortensen, A., Moskowitz, R., and R. K., "Distributed Denial of Service (DDoS) Open Threat Signaling Requirements", draft-ietf-dots-requirements-16 (work in progress), October 2018.

Authors’ Addresses

Kaname Nishizuka (editor)
NTT Communications
GranPark 16F 3-4-1 Shibaura, Minato-ku
Tokyo  108-8118
Japan

Email: kaname@nttv6.jp

Takahiko Nagata
Lepidum
Japan

Email: nagata@lepidum.co.jp

Tirumaleswar Reddy (editor)
McAfee, Inc.
Embassy Golf Link Business Park
Bangalore, Karnataka  560071
India

Email: kondtir@gmail.com

Mohamed Boucadair
Orange
Rennes  35000
France

Email: mohamed.boucadair@orange.com