DOTS T. Reddy
Internet-Draft McAfee
Intended status: Standards Track M. Boucadair
Expires: October ~~26,~~ **28,** 2019 Orange
J. Shallow
April ~~24,~~ **26,** 2019

Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Call Home

~~draft-ietf-dots-signal-call-home-00~~
draft-ietf-dots-signal-call-home-01

Abstract

This document ~~presents~~ **specifies the** DOTS signal channel Call Home service, which enables a DOTS server to initiate a secure connection to a DOTS client, and to receive the attack traffic information from the DOTS client. The DOTS server in turn uses the attack traffic information to identify the compromised devices launching the outgoing DDoS attack and takes appropriate mitigation ~~action.~~ **action(s).**

The Call Home service is not specific to the home networks; the solution targets any deployment which requires to block DDoS attack traffic closer to the source(s) of a DDoS attack.

Status of This Memo

This Internet-Draft will expire on October ~~26,~~ **28,** 2019.

Copyright Notice

Table of Contents

1. Introduction

1.1. The Problem

The DOTS signal channel protocol [I-D.ietf-dots-signal-channel] is used to carry information about a network resource or a network (or a part thereof) that is under a Distributed Denial of Service (DDoS) attack. Such information is sent by a DOTS client to one or multiple DOTS servers so that appropriate mitigation actions are undertaken on traffic deemed suspicious. Various use cases are discussed in [I-D.ietf-dots-use-cases].

~~IoT~~

Internet of Things (IoT) devices are becoming more and more prevalent in home networks, and with compute and memory becoming cheaper and cheaper, various types of IoT devices become available in the consumer market at affordable price. But on the downside, the main threat being most of these IoT devices are bought off-the-shelf and most manufacturers haven't considered security in the product design. IoT devices deployed in home networks can be easily compromised, they do not have an easy mechanism to upgrade, and IoT manufactures may cease manufacture and/or discontinue patching vulnerabilities on IoT ~~devices.~~ **devices (Section 5.4 of [I-D.irtf-t2trg-iot-seccons]).** However, these vulnerable and compromised devices will continue **to** be used for a long period of time in the home, and the ~~end-user~~ **end-user** does not know that IoT devices in his/her home are compromised. The compromised IoT devices are typically used for launching DDoS attacks **(Section 3 of [I-D.irtf-t2trg-iot-seccons])** on ~~the victim~~ **victims** while the ~~owner/administrator~~ **owner/administrator** of the home network is not aware about such misbehaviors. Similar to other DDoS attacks, the victim in this attack can be an application server, a host, a router, a firewall, or an entire network.

Nowadays, network devices in a home network offer network ~~security, for instance, firewall/IPS~~ **security (e.g., firewall or Intrusion Protection System (IPS)** service on a home ~~router or gateway~~ **router)** to protect the devices connected to the home network from **both** external and internal attacks. Over the years several techniques have been identified to detect DDoS attacks, some of these techniques can be enabled on home network devices but most of them are used in the Internet Service Provider (ISP)'s network. The ISP offering DDoS mitigation service can detect outgoing DDoS attack traffic originating from its subscribers or the ISP may receive filtering rules ~~(for example,~~ **(e.g.,** using BGP flowspec [RFC5575]) from **a** downstream service provider to filter, block, or rate-limit DDoS attack traffic originating from the ISP's subscribers to ~~the~~ **a** downstream target.

Some of the DDoS attacks like spoofed RST or FIN packets, Slowloris, and ~~TLS~~ **Transport Layer Security (TLS)** re-negotiation are difficult to detect on ~~the~~ **a** home network ~~devices~~ **device** without adversely affecting its performance. The reason is typically home **devices such as home** routers have fast path to boost the throughput. For every new ~~TCP/UDP~~ **TCP/UDP** flow, only the first few packets are punted through the slow path. Hence, it is not possible to detect various DDoS attacks in the slow path, since the attack payload is sent to the target server after the flow is switched to fast path. Deep ~~packet inspection~~ **Packet Inspection** (DPI) of all the packets of a flow would be able to detect some of the attacks. However, a full-fledged DPI to detect these type of DDoS attacks is functionally or operationally not possible for all the devices attached to the home network owing to the memory and CPU limitations of the home routers. Further, for certain DDoS attacks the ability to distinguish legitimate traffic from attacker traffic on a per packet basis is complex. This complexity ~~originates from the fact~~ **is due to** that the packet itself may look "legitimate" and no attack signature can be identified. The anomaly can be identified only after detailed statistical analysis.

The ISP on the other hand can detect ~~the~~ **some** DDoS ~~attack~~ **attacks** originating from a home ~~network,~~ **network (Section 2.6 of [RFC8517]),** but the ISP does not have a mechanism to detect which device in the home network is generating the DDoS attack traffic. The primary reason being that devices in ~~a~~ **an** IPv4 ~~Home~~ **home** network are typically behind a ~~NAT~~ **Network Address Translation (NAT)** border. Even in case of a IPv6 ~~Home~~ **home** network, although the ISP can identify the infected device in the ~~Home~~ **home** network launching the DDoS traffic by tracking its unique IPv6 address, the infected device can easily change ~~the IP~~ **its IPv6** address to evade remediation.

Existing approaches are still suffering from misused access network resources by abusing devices; the support of means for blocking such attacks close to the sources are missing. In particular, the DOTS signal protocol does not discuss cooperative DDoS mitigation between the ~~home~~ network **hosting an attack source** and **the** ISP to the suppress the outbound DDoS attack traffic originating from ~~the home~~ **that** network.

1.2. The Solution

This specification addresses the problems discussed in Section 1.1 and presents **the** DOTS signal channel Call Home extension, which enables the DOTS server to initiate a secure connection to the DOTS client, and the DOTS client then conveys the attack traffic information to the DOTS server.

A DOTS client relies upon a variety of triggers to invoke the Call Home function (e.g., scrubbing the traffic from the attack source, receiving an alert from an attack target, a peer DDoS Mitigation System (DMS), or a transit provider). The definition of these triggers is deployment-specific. It is therefore out of the scope of this document to elaborate on how these triggers are made available to a DOTS client.

In a typical deployment scenario, the DOTS server is enabled on a ~~CPE,~~ **Customer Premises Equipment (CPE),** which is aligned with recent trends to enrich the CPE with advanced security features. Unlike classic DOTS deployments [I-D.ietf-dots-use-cases], such DOTS server maintains a single DOTS signal channel session for each DOTS-capable upstream provisioning domain [I-D.ietf-dots-multihoming].

For instance, the DOTS server in the home network initiates the Call Home in 'idle' time and then subsequently the DOTS client in the ISP environment can initiate a mitigation request whenever the ISP detects there is an attack from a compromised device in the DOTS server ~~domain.~~ **domain (i.e., from within the home network).**

The DOTS server uses the DDoS attack traffic information to identify the compromised device in its domain **that is responsible for** launching the DDoS attack, notifies ~~the~~ **eventually a** network administrator, and takes appropriate mitigation ~~action. The~~ **action(s). A** mitigation action can be to quarantine the compromised device or block its traffic to the attack ~~target~~ **target(s)** until the mitigation request is withdrawn.

Other motivations for introducing the Call Home function are discussed in Section 1.1 of [RFC8071].

This document assumes that DOTS servers are provisioned with a way to know how to reach the upstream DOTS client(s), which could occur by a variety of means (e.g., [I-D.ietf-dots-server-discovery]). The specification of such means are out of scope of this document.

1.3. **Applicability** Scope

The aforementioned problems may be encountered in other deployments than those discussed in Section ~~1.1.~~ **1.1 (e.g., data centers, enterprise networks).** The solution specified in this document can be used for those deployments to block DDoS attack traffic closer to the source(s) of the attack. **The Call Home reference architecture is shown in Figure 1.**

```
                 Attack Target
                      | /\
                      | ||
......................|.||....................
                      | ||
             .--------+-||-------.
            (           ||        )-.
```

```
             .'            ||           '
             (  Internet   ||            )
              (            ||          -'
               '-(         ||          )
                  '------+-||---------'
   ......................|.||.....................
                         | ||   Service Provider
                .--------+-||-------.
               (           ||        )-.
             .' DOTS       ||           '
             ( Client      ||            )
              (            ||          -'
               '-(         ||          )
                  '------+-||---------'
                         | ||
   ......................|.||.......................
                         | ||    Source Network
                .--------+-||-------.
               (           ||        )-.
             .' DOTS       ||           '
             ( Server      || Outbound   )
              (            ||   DDoS   -'
               '-(         ||  Attack  )
                  '------+-||---------'
                         | ||
                         | ||
                    Attack Source
```

Figure 1: Call Home Reference Architecture

It is out of the scope of this document to identify an exhaustive list of such deployments.

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].

The meaning of the symbols in YANG tree diagrams is defined in [RFC8340].

(D)TLS is used for statements that apply to both Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). Specific terms are used for any statement that applies to either protocol alone.

3. DOTS Signal Channel Call Home

3.1. Procedure

The DOTS signal channel Call Home extension preserves all but one of the DOTS client/server roles in the DOTS protocol stack, as compared to DOTS client-initiated DOTS signal channel protocol [I-D.ietf-dots-signal-channel]. The ~~one and only~~ role reversal that occurs are at the ~~TLS or DTLS layers;~~ **(D)TLS layer;** that is, **(1)** the DOTS server acts as a DTLS client and the DOTS client acts as a DTLS server or **(2)** the DOTS server acts as a TLS client **initiating the underlying TCP connection** and the DOTS client acts as a TLS server. The DOTS server initiates ~~TLS handshake or DTLS~~ **(D)TLS** handshake to the DOTS client.

For example, a home network element (e.g., home router) co-located with a DOTS server (likely, a client-domain DOTS gateway) is the ~~TLS server and DTLS~~ **(D)TLS** server. However, when calling home, the DOTS server initially assumes the role of the ~~TLS client and DTLS~~ **(D)TLS** client, but the network element's role as a DOTS server remains the same. Furthermore, existing certificate chains and mutual authentication mechanisms between the DOTS agents are unaffected by the Call Home function. This Call Home function enables the DOTS server co-located with a network element (possibly behind NATs and firewalls) reachable by only the intended DOTS client and hence the DOTS server cannot be subjected to DDoS attacks. ~~Other motivations for introducing the Call Home function are discussed in Section 1.1 of [RFC8071].~~

~~This document assumes that DOTS servers are provisioned with a way to~~

~~know how to reach the upstream DOTS client(s), which could occur by a variety of means (e.g., [I-D.ietf-dots-server-discovery]). The specification of such means are out of scope of this document.~~

Figure ~~1~~ **2** illustrates a sample Call Home flow exchange:

```
           DOTS                               DOTS
          ~~Server~~                             ~~Client~~
          server                             client
            |                                  |
            |         1. (D)TLS connection     |
            |--------------------------------->|
            |         2. Mitigation request    |
            |<---------------------------------|
            |                ...               |
```

Figure ~~1:~~ **2:** DOTS Signal Channel Call Home Sequence Diagram

The **DOTS signal channel** Call Home procedure is as follows:

1. If UDP transport is used, the DOTS server begins by initiating a DTLS connection to the DOTS client. The DOTS client MUST support accepting DTLS connection on the IANA-assigned port number defined in Section 4.1, but MAY be configured to listen to a different port number.

   If TCP is used, the DOTS server begins by initiating a TCP connection to the DOTS client. The DOTS client MUST support accepting TCP connections on the IANA-assigned port number defined in Section 4.1, but MAY be configured to listen to a different port number. Using this TCP connection, the DOTS server initiates a TLS connection to the DOTS client.

   The Happy Eyeballs mechanism explained in Section 4.3 of [I-D.ietf-dots-signal-channel] can be used for initiating (D)TLS connections.

2. Using this (D)TLS connection, the DOTS client may request, withdraw, or retrieve the status of mitigation requests.

3.2. DOTS Signal Channel Extension

3.2.1. Mitigation Request

This specification extends the mitigation request defined in **Section 4.4.1 of** [I-D.ietf-dots-signal-channel] to convey the attacker source prefixes and source port numbers. The DOTS client conveys the following new parameters in the CBOR body of the mitigation request:

source-prefix: A list of attacker prefixes used to attack the target. Prefixes are represented using Classless Inter-Domain Routing (CIDR) notation [RFC4632].

As a reminder, the prefix length MUST be less than or equal to 32 (resp. 128) for IPv4 (resp. IPv6).

The prefix list MUST NOT include broadcast, loopback, or multicast addresses. These addresses are considered as invalid values. In addition, the DOTS client MUST validate that attacker prefixes are within the scope of the DOTS server domain.

This is an optional attribute.

source-port-range: A list of port numbers used by the attack traffic flows.

A port range is defined by two bounds, a lower port number (lower-port) and an upper port number (upper-port). When only 'lower-port' is present, it represents a single port number.

For TCP, UDP, Stream Control Transmission Protocol (SCTP) [RFC4960], or Datagram Congestion Control Protocol (DCCP) [RFC4340], a range of ports can be, for example, 0-1023, 1024-65535, or 1024-49151.

This is an optional attribute.

source-icmp-type: A list of ICMP types used by the attack traffic flows. An ICMP type range is defined by two bounds, a lower ICMP type (lower-type) and an upper ICMP type (upper-type). When only 'lower-type' is present, it represents a single ICMP type.

This is an optional attribute.

The 'source-prefix' parameter is a mandatory attribute when the attack traffic information is signaled by a DOTS client in the Call Home scenario. The 'target-uri' or 'target-fqdn' parameters can be included in a mitigation request for diagnostic purposes to notify the DOTS server domain administrator, but SHOULD NOT be used to determine the target IP addresses. Note that 'target-prefix' becomes a mandatory attribute in the mitigation request signaling the attack information because 'target-uri' and 'target-fqdn' are optional attributes and 'alias-name' will not be conveyed in a mitigation request.

In order to help attack source identification by a DOTS server, the DOTS client SHOULD include in its mitigation request additional information such as 'source-port-range' or 'source-icmp-type-range'. The DOTS client may not include such information if 'source-prefix' conveys an IPv6 address/prefix.

If a Carrier Grade NAT (CGN, including NAT64) is located between the DOTS client domain and DOTS server domain, communicating an external IP address in a mitigation request is likely to be discarded by the DOTS server because the external IP address is not visible locally to the DOTS server. The DOTS server is only aware of the internal IP addresses/prefixes bound to its domain. Thus, the DOTS client MUST NOT include the external IP address and/or port number identifying the suspect attack source, but MUST include the internal IP address and/or port number. To that aim, the DOTS client SHOULD rely on mechanisms, such as [RFC8512] or [RFC8513], to retrieve the internal IP address and port number which are mapped to an external IP address and port number.

If a MAP Border Relay [RFC7597] or lwAFTR [RFC7596] is enabled in the provider's domain to service its customers, the identification of an attack source bound to an IPv4 address/prefix MUST also rely on source port numbers because the same IPv4 address is assigned to multiple customers. The port information is required to unambiguously identify the source of an attack.

The DOTS server MUST check that the 'source-prefix' is within the scope of the DOTS server domain in the Call Home scenario. Note that in such scenario, the DOTS server considers, by default, that any routeable IP prefix is within the scope of the DOTS client. Invalid mitigation requests are handled as per Section 4.4.1 of [I-D.ietf-dots-signal-channel].

If a translator is enabled on the boundaries of the domain hosting the DOTS server (a CPE with NAT enabled, typically), the DOTS server uses the attack traffic information conveyed in a mitigation request to find the internal source IP address of the compromised device and blocks the traffic from the compromised device traffic to the attack target until the mitigation request is withdrawn. Doing so allows to isolate the suspicious device while avoiding to disturb other services.

The DOTS server domain administrator consent MAY be required to block the traffic from the compromised device to the attack target. An implementation MAY have a configuration knob to block the traffic from the compromised device to the attack target with or without DOTS server domain administrator consent. If the attack traffic is blocked, the DOTS server informs the DOTS client that the attack is being mitigated.

If the attack traffic information is identified by the DOTS server or the DOTS server domain administrator as legitimate traffic, the mitigation request is rejected, and 4.09 (Conflict) is returned to the DOTS client. The conflict-clause (defined in Section 4.4.1 of [I-D.ietf-dots-signal-channel]) indicates the cause of the conflict. The following new value is defined:

4: Mitigation request rejected. This code is returned by the DOTS server to indicate the attack traffic has been classified as legitimate traffic.

~~If~~

Once the request is validated by the DOTS server, appropriate actions

are enforced to block the attack traffic within the source network. The DOTS client is informed about the progress of the attack mitigation following the rules in [I-D.ietf-dots-signal-channel]. For example, if the DOTS server is ~~co-located with~~ **embedded in** a ~~home router,~~ **CPE,** it can program the packet processor to punt all the traffic from the compromised device to the target to slow path. The ~~home router~~ **CPE** inspects the punted slow path traffic to detect and block the outgoing DDoS attack traffic or quarantine the device (e.g., using MAC level filtering) until it is remediated, and notifies the ~~home~~ **CPE** administrator about the compromised device.

3.2.2. DOTS Signal Call Home YANG 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 signaling the attack traffic information. This document defines the YANG module "ietf-dots-call-home", which has the following tree structure:

```
module: ietf-dots-call-home
  augment /ietf-signal:dots-signal/ietf-signal:message-type
          /ietf-signal:mitigation-scope/ietf-signal:scope:
    +--rw source-prefix*     inet:ip-prefix {source-signaling}?
    +--rw source-port-range*
    ~~|  |             [lower-port upper-port]~~ [lower-port] {source-signaling}?
    |  +--rw lower-port    inet:port-number
    |  +--rw ~~upper-port~~ upper-port?   inet:port-number
    +--rw source-icmp-type-range*
       |           ~~[lower-type upper-type]~~                    [lower-type] {source-signaling}?
       +--rw lower-type    uint8
       +--rw ~~upper-type~~ upper-type?   uint8
```

3.2.2.2. YANG Module

This module uses the common YANG types defined in [RFC6991].

<CODE BEGINS> file ~~"ietf-dots-call-home@2018-04-01.yang"~~ **"ietf-dots-call-home@2019-04-25.yang"**

```
module ietf-dots-call-home {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-dots-call-home";
  prefix call-home;

  import ietf-inet-types {
    prefix inet;
    reference
      "Section 4 of RFC 6991";
  }
  import ietf-dots-signal-channel {
    prefix ietf-signal;
    reference
      "RFC YYYY: Distributed Denial-of-Service Open Threat
                 Signaling (DOTS) Signal Channel Specification";
  }

  organization
    "IETF DDoS Open Threat Signaling (DOTS) Working Group";
  contact
    "WG Web:   <https://datatracker.ietf.org/wg/dots/>
     WG List:  <mailto:dots@ietf.org>

     Editor:  Konda, Tirumaleswar Reddy
              <mailto:TirumaleswarReddy_Konda@McAfee.com>;

     Editor:  Mohamed Boucadair
              <mailto:mohamed.boucadair@orange.com>;

     Editor:  Jon Shallow
              <mailto:ietf-supjps@jpshallow.com>";

  description
    "This module contains YANG ~~definition~~ definitions for the signaling
     messages exchanged between a DOTS client and a DOTS server
     for the ~~call home~~ Call Home deployment scenario.

     Copyright (c) ~~2018~~ 2019 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 ~~2018-04-01~~ 2019-04-25 {
    description
      "Initial revision.";
    reference
      "RFC XXXX: Distributed Denial-of-Service Open Threat
                 Signaling (DOTS) Signal Channel Call Home";
  }

  feature source-signaling {
    description
      "This feature means that source-related information
       can be supplied in mitigation requests.";

  }

  augment "/ietf-signal:dots-signal/ietf-signal:message-type/"
        + "ietf-signal:mitigation-scope/ietf-signal:scope" {
    if-feature source-signaling;
    description "Attacker source ~~details";~~ details.";

    leaf-list source-prefix {
      type inet:ip-prefix;
      description
        "IPv4 or IPv6 prefix identifying the attacker(s).";
    }
    list source-port-range {
      key ~~"lower-port upper-port";~~ "lower-port";
      description
        "Port range. When only lower-port is
         present, it represents a single port number.";
      leaf lower-port {
        type inet:port-number;
        mandatory true;
        description
          "Lower port number of the port range.";
      }
      leaf upper-port {
        type inet:port-number;
        must ". >= ../lower-port" {
           error-message
             "The upper port number must be greater than
              or equal to lower port number.";
        }
        description
          "Upper port number of the port range.";
      }
    }
    list source-icmp-type-range {
      key ~~"lower-type upper-type";~~ "lower-type";
      description
        "ICMP type range. When only lower-type is
         present, it represents a single ICMP type.";
      leaf lower-type {
        type uint8;
        mandatory true;
        description
          "Lower ICMP type of the ICMP type range.";
      }
      leaf upper-type {
        type uint8;
        must ". >= ../lower-type" {
           error-message
             "The upper ICMP type must be greater than
             or equal to lower ICMP type.";
        }
        description
          "Upper type of the ICMP type range.";
      }
    }
  }
}
```

<CODE ENDS>

4. IANA Considerations

4.1. DOTS Signal Channel Call Home UDP and TCP Port Number

IANA is requested to assign the port number TBD to the DOTS signal channel Call Home protocol for both UDP and TCP from the "Service Name and Transport Protocol Port Number Registry" available at: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.

The assignment of port number 4647 is strongly suggested (DOTS signal channel uses port number 4646).

4.2. DOTS Signal Channel CBOR Mappings Registry

This specification registers the 'source-prefix' and 'source-port-range' parameters in the IANA "DOTS Signal Channel CBOR Mappings" registry established by [I-D.ietf-dots-signal-channel].

The 'source-prefix', 'source-port-range', and 'source-icmp-type-range' are comprehension-optional parameters.

- o Note to the RFC Editor: Please delete (TBD1)-(TBD5) once CBOR keys are assigned from the 0x8000 - 0xBFFF range.

Parameter Name	YANG Type	CBOR Key	CBOR Major Type & Information	JSON Type
source-prefix	leaf-list inet: ip-prefix	0x8000 (TBD1)	4 array 3 text string	Array String
source-port-range	list	0x8001 (TBD2)	4 array	Array
source-icmp-type-range	list	0x8002 (TBD3)	4 array	Array
lower-type	uint8	0x8003 (TBD4)	0 unsigned	Number
upper-type	uint8	0x8004 (TBD5)	0 unsigned	Number

4.3. New DOTS Conflict Cause

This document requests IANA to assign a new code from the "DOTS Conflict Cause Codes" registry:

Code	Label	Description	Reference
4	request-rejected	Mitigation request rejected. This code is returned by the DOTS server to indicate the attack traffic has been classified as legitimate traffic.	[RFCXXXX]

4.4. DOTS Signal Call Home YANG Module

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

URI: urn:ietf:params:xml:ns:yang:ietf-dots-call-home
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].

Name: ietf-call-home
Namespace: urn:ietf:params:xml:ns:yang:ietf-dots-call-home
Maintained by IANA: N
Prefix: call-home
Reference: RFC XXXX

5. Security Considerations

This document deviates from classic DOTS signal channel usage by having the DOTS server initiate the TLS or DTLS connection. DOTS signal channel related security considerations discussed in Section 10 of [I-D.ietf-dots-signal-channel] MUST be considered. DOTS agents MUST authenticate each other using (D)TLS before a DOTS signal channel session is considered valid.

An attacker may launch a DoS attack on the DOTS client by having it perform computationally expensive operations, before deducing that the attacker doesn't possess a valid key. For instance, in TLS 1.3 [RFC8446], the ServerHello message contains a Key Share value based on an expensive asymmetric key operation for key establishment. Common precautions mitigating DoS attacks are recommended, such as temporarily blacklisting the source address after a set number of unsuccessful authentication attempts.

DOTS servers may not blindly trust mitigation requests from DOTS clients. For example, DOTS servers can use the attack flow information in a mitigation request to enable full-fledged packet inspection function to inspect all the traffic from the compromised to the target or to re-direct the traffic from the compromised device to the target to a DDoS mitigation system to scrub the suspicious traffic. DOTS servers can also seek the consent of DOTS server domain administrator to block the traffic from the compromised device to the target (see Section 3.2.1).

6. Privacy Considerations

The considerations discussed in [RFC6973] were taken into account to assess whether the DOTS Call Home extension introduces privacy threats.

Concretely, the protocol does not leak any new information that can be used to ease surveillance. In particular, the DOTS server is not required to share information that is local to its network (e.g., internal identifiers of an attack source) with the DOTS client.

The DOTS Call Home extension does not preclude the validation of mitigation requests received from a DOTS client. For example, a security service running on the CPE may require administrator's consent before the CPE acts upon the mitigation request indicated by the DOTS client. How the consent is obtained is out of scope of this document.

Note that a DOTS server can seek for an administrator's consent, validate the request by inspecting the traffic, or proceed with both.

The DOTS Call Home extension is only advisory in nature. Concretely, the DOTS Call Home extension does not impose any action to be enforced within the home network; it is up to the DOTS server (and/or network administrator) to decide whether and which actions are required.

Moreover, the DOTS Call Home extension avoids misattribution by appropriately identifying the network to which a suspect attack source belongs to (e.g., address sharing issues discussed in Section 3.2.1).

Triggers to send a DOTS mitigation request to a DOTS server are deployment-specific. For example, a DOTS client may rely on the output of some DDoS detection systems deployed within the DOTS ~~client's network~~ **client domain** to detect potential outbound DDoS attacks or on abuse claims received from remote victim networks. Such DDoS detection and mitigation techniques are not meant to track the activity of users, but to protect the Internet and avoid altering the IP reputation of the DOTS ~~client's~~ **client** domain.

7. Contributors

The following individuals have contributed to this document:

Joshi Harsha
McAfee, Inc.
Embassy Golf Link Business Park
Bangalore, Karnataka 560071
India

Email: harsha_joshi@mcafee.com

8. Acknowledgements

Thanks to Wei Pei, Xia Liang, Roman Danyliw, Dan Wing, Toema Gavrichenkov, Daniel Migault, and Valery Smyslov for the comments.

9. References

9.1. Normative References

[I-D.ietf-dots-signal-channel]
K, R., Boucadair, M., Patil, P., Mortensen, A., and N. Teague, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Specification", draft-ietf-dots-signal-channel-31 (work in progress), March 2019.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <https://www.rfc-editor.org/info/rfc3688>.

[RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6991, DOI 10.17487/RFC6991, July 2013, <https://www.rfc-editor.org/info/rfc6991>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

9.2. Informative References

[I-D.ietf-dots-multihoming]
Boucadair, M. and R. K, "Multi-homing Deployment Considerations for Distributed-Denial-of-Service Open Threat Signaling (DOTS)", draft-ietf-dots-multihoming-01 (work in progress), January 2019.

[I-D.ietf-dots-requirements]
Mortensen, A., K, R., and R. Moskowitz, "Distributed Denial of Service (DDoS) Open Threat Signaling Requirements", draft-ietf-dots-requirements-22 (work in progress), March 2019.

[I-D.ietf-dots-server-discovery]
Boucadair, M., K, R., and P. Patil, "Distributed-Denial-of-Service Open Threat Signaling (DOTS) Server Discovery", draft-ietf-dots-server-discovery-01 (work in progress), April 2019.

[I-D.ietf-dots-use-cases]
Dobbins, R., Migault, D., Fouant, S., Moskowitz, R., Teague, N., Xia, L., and K. Nishizuka, "Use cases for DDoS Open Threat Signaling", draft-ietf-dots-use-cases-17 (work in progress), January 2019.

**[I-D.irtf-t2trg-iot-seccons]
Garcia-Morchon, O., Kumar, S., and M. Sethi, "State-of-the-Art and Challenges for the Internet of Things Security", draft-irtf-t2trg-iot-seccons-16 (work in progress), December 2018.**

[RFC4340] Kohler, E., Handley, M., and S. Floyd, "Datagram Congestion Control Protocol (DCCP)", RFC 4340, DOI 10.17487/RFC4340, March 2006, <https://www.rfc-editor.org/info/rfc4340>.

[RFC4632] Fuller, V. and T. Li, "Classless Inter-domain Routing

(CIDR): The Internet Address Assignment and Aggregation Plan", BCP 122, RFC 4632, DOI 10.17487/RFC4632, August 2006, <https://www.rfc-editor.org/info/rfc4632>.

[RFC4732] Handley, M., Ed., Rescorla, E., Ed., and IAB, "Internet Denial-of-Service Considerations", RFC 4732, DOI 10.17487/RFC4732, December 2006, <https://www.rfc-editor.org/info/rfc4732>.

[RFC4960] Stewart, R., Ed., "Stream Control Transmission Protocol", RFC 4960, DOI 10.17487/RFC4960, September 2007, <https://www.rfc-editor.org/info/rfc4960>.

[RFC5575] Marques, P., Sheth, N., Raszuk, R., Greene, B., Mauch, J., and D. McPherson, "Dissemination of Flow Specification Rules", RFC 5575, DOI 10.17487/RFC5575, August 2009, <https://www.rfc-editor.org/info/rfc5575>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.

[RFC7596] Cui, Y., Sun, Q., Boucadair, M., Tsou, T., Lee, Y., and I. Farrer, "Lightweight 4over6: An Extension to the Dual-Stack Lite Architecture", RFC 7596, DOI 10.17487/RFC7596, July 2015, <https://www.rfc-editor.org/info/rfc7596>.

[RFC7597] Troan, O., Ed., Dec, W., Li, X., Bao, C., Matsushima, S., Murakami, T., and T. Taylor, Ed., "Mapping of Address and Port with Encapsulation (MAP-E)", RFC 7597, DOI 10.17487/RFC7597, July 2015, <https://www.rfc-editor.org/info/rfc7597>.

[RFC8071] Watsen, K., "NETCONF Call Home and RESTCONF Call Home", RFC 8071, DOI 10.17487/RFC8071, February 2017, <https://www.rfc-editor.org/info/rfc8071>.

[RFC8340] Bjorklund, M. and L. Berger, Ed., "YANG Tree Diagrams", BCP 215, RFC 8340, DOI 10.17487/RFC8340, March 2018, <https://www.rfc-editor.org/info/rfc8340>.

[RFC8512] Boucadair, M., Ed., Sivakumar, S., Jacquenet, C., Vinapamula, S., and Q. Wu, "A YANG Module for Network Address Translation (NAT) and Network Prefix Translation (NPT)", RFC 8512, DOI 10.17487/RFC8512, January 2019, <https://www.rfc-editor.org/info/rfc8512>.

[RFC8513] Boucadair, M., Jacquenet, C., and S. Sivakumar, "A YANG Data Model for Dual-Stack Lite (DS-Lite)", RFC 8513, DOI 10.17487/RFC8513, January 2019, <https://www.rfc-editor.org/info/rfc8513>.

[RFC8517] Dolson, D., Ed., Snellman, J., Boucadair, M., Ed., and C. Jacquenet, "An Inventory of Transport-Centric Functions Provided by Middleboxes: An Operator Perspective", RFC 8517, DOI 10.17487/RFC8517, February 2019, <https://www.rfc-editor.org/info/rfc8517>.

Authors' Addresses

Tirumaleswar Reddy
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

Jon Shallow
UK

Email: supjps-ietf@jpshallow.com