DOTS T. Reddy
Internet-Draft ~~J. Harsha~~ McAfee
Intended status: Standards Track ~~McAfee~~ M. Boucadair
Expires: April 1, 2019 Orange
J. Harsha
McAfee
September 28, 2018

Denial-of-Service Open Threat Signaling (DOTS) Signal ~~Channel~~ and Data Channels Call Home

draft-reddy-dots-home-network-00

Abstract

This document presents DOTS ~~signal channel~~ Call ~~Home,~~ Home service, which enables a DOTS ~~server~~ agent to initiate a secure connection to a DOTS ~~client,~~ peer, and to convey the attack traffic information ~~to~~ from the DOTS ~~server.~~ peer (acting as a DOTS server). 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.

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 ~~device~~ **network resource** or a network (or a part thereof) that is under a ~~DDoS~~ **Distributed Denial of Service (DDoS)** attack. Such information is sent by a DOTS client to ~~an upstream~~ **one or multiple** DOTS ~~server~~ **servers** so that appropriate mitigation actions are undertaken on traffic deemed suspicious. **Likewise, the DOTS data channel protocol [I-D.ietf-dots-data-channel] is used to install filtering rules that may be instantiated immediately or when an attack is encountered. Various use cases are discussed in [I-D.ietf-dots-use-cases].**

IoT devices are becoming more and more prevalent in ~~Home~~ **home** networks, and with compute and memory becoming cheaper and cheaper, various types of IoT devices are 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~~ **off-the-shelf** and most manufacturers haven't considered security in the product design. IoT devices deployed in ~~Home~~ **home** networks can be easily compromised, they do not have easy mechanism to upgrade, and IoT manufactures may shut shop and discontinue patching vulnerabilities on IoT devices. However, these vulnerable and compromised devices will continue be used for a long period of time in the home, and the end-user does not know that IoT devices in his/her home are compromised. The compromised IoT devices are typically used for launching ~~Distributed denial of service (DDoS)~~ **DDoS** attacks on the ~~victim. The~~ **victim while the owner/administrator of the home network is not aware about such misbehaviors. Similar to other DDoS attack, the** victim in this attack can be an application server, a host, a router, a firewall, or an entire network.

~~Now-a-days,~~

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

Some of the DDoS attacks like spoofed RST or FIN packets, ~~Slowloris~~ **Slowloris,** and TLS re-negotiation are difficult to detect on the home network devices without adversely affecting its performance. The reason is typically home routers have fast path to boost the throughput. For every new 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 (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 operationally not possible for all the devices attached to the ~~Home~~ **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 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 DDoS attack originating from a ~~Home~~ **home** network, but the ISP does not have a mechanism to detect which device in the ~~Home~~ **home** network is generating the DDoS attack traffic. The primary reason being devices in a IPv4 Home network are behind NAT. Even in case of a IPv6 Home network, though the ISP can identify the infected device in the Home network launching the DDoS traffic using its unique IPv6 ~~address~~ **address,** but the infected device can easily change the IP address to evade remediation.

Also, the DDoS mitigation service enabled at the ISP network does not know whether some traffic is consented or is a suspicious one; this may be exacerbated by the unavailability of some control messages used by emerging transport protocol (and which were used to be sent in clear in TCP, for example). The lack for a clear consent message and its association with packets belong to that flow make impose some additional requirement on how suspects packets have to be processed by the ISP while increasing the security of its own infrastructure and avoid negative reputation of its IP resources if more and more machines, known to be source of DDoS, are hosted in its network.

Existing approaches are still suffering from misusing 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~~ **signal/data** channel ~~protocol does~~ **protocols do** not discuss cooperative DDoS mitigation between the ~~Home~~ **home** network and ISP to the suppress the outbound DDoS attack traffic originating from the ~~Home~~ **home** network.

1.2. The Solution

This specification addresses ~~this problem~~ **the problems discussed in Section 1.1** and presents DOTS ~~signal~~ **signal/data** channel Call Home ~~protocol,~~ **extension,** which enables the DOTS server to initiate a secure connection to the DOTS client, and the DOTS client conveys the attack traffic information to the DOTS server. The DOTS server uses the DDoS attack traffic information to identify the compromised device launching the DDoS attack, notifies the network ~~administrator~~ **administrator,** and takes appropriate mitigation action. The mitigation action can be to quarantine the compromised device or block its traffic to the attack target until

the mitigation request is withdrawn.

~~2. Notational Conventions and Terminology~~

~~The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",~~

Abuse traffic can be filtered at the boundaries of the home network or at the ISP network. This document defines means to allow for both deployment models.

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 ~~[RFC2119].~~ **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. DOTS Signal Channel Call Home

3.1. Procedure

DOTS signal channel Call Home 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. The one and only role reversal that occurs are at the TCP/TLS and DTLS layers; that is, the DOTS server acts as a DTLS client and the DOTS client acts as a DTLS server or the ~~the~~ DOTS server acts as a TCP/TLS client and the DOTS client acts as a TCP/TLS server. The DOTS server initiates TCP/TLS handshake or DTLS handshake to the DOTS client.

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

~~The diagram below~~

Figure 1 illustrates ~~call home from a protocol layering perspective:~~ **sample Call Home flow exchange:**

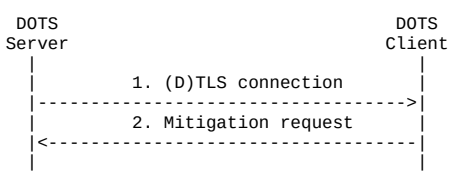

Figure 1: **Signal Channel** Call Home Sequence Diagram

This diagram makes the following points:

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 defined in Section 5.1, but MAY be configured to listen to a different port. If TCP ~~transport~~ is used, the DOTS server begins by initiating a TCP connection to the DOTS ~~server.~~ **client.** The DOTS client MUST support accepting TCP ~~connection~~ **connections** on the IANA-assigned port defined in Section 5.1, but MAY be configured to listen to a different port. Using this TCP connection, the DOTS server initiates an TLS connection to the DOTS client.

2. Using this (D)TLS connection, the DOTS client requests, withdraws, or retrieves the status of mitigation requests.

~~4.~~

3.2. DOTS Signal Channel Extension

~~4.1.~~

3.2.1. Mitigation ~~request~~ **Request**

This specification extends the mitigation request defined in [I-D.ietf-dots-signal-channel] to convey the attacker source prefixes and source ~~ports.~~ **port numbers.** The DOTS client in the mitigation request 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~~ **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~~ **values. In** addition, the DOTS client MUST validate that attacker prefixes are within the scope of the DOTS server's 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.

   The 'source-prefix', 'source-port-range', 'target-prefix', 'target-
   port-range', and 'target-protocol' parameters are mandatory
   attributes when the attack traffic information is signaled by the
   DOTS client.

   The DOTS server uses the attack traffic information to find the pre-
   NAT 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.  The DOTS server informs
   the DOTS client that the attack traffic is blocked.

   If the DOTS server is co-located with a home router, it can program
   the packet processor to punt all the traffic from the compromised
   device to the target to slow path.  The home router inspects the
   punted slow path traffic to detect and block the outgoing DDoS attack
   traffic or quarantine the device ~~(e.g.~~ (e.g., using MAC level filtering)
   until it is remediated, and notify the home administrator about the
   compromised device.

   If the DOTS server is co-located with a home router is not able to
   enforce appropriate filtering rules within the local network, the
   DOTS server (acting now as a DOTS client) may use the DOTS data
   channel to request explicit filtering from the peer DOTS agent.

   TBD: Do we also want to convey Attack Name/type or ID (the home
   router may not be capable of detecting new emerging/sophisticated
   attacks) ?

~~4.2.~~

3.2.2.  DOTS Signal Call Home YANG ~~Model~~

~~4.2.1.~~ Module

3.2.2.1.  Mitigation Request ~~Model structure~~ 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~~ defines the YANG module
   "ietf-dots-signal-call-home", which has the following structure:

   module: ietf-dots-signal-call-home
     augment /ietf-signal:dots-signal:
       +--rw source-prefix*       inet:ip-prefix
       +--rw source-port-range* [lower-port upper-port]
          +--rw lower-port    inet:port-number
          +--rw upper-port    inet:port-number

3.2.2.2.  Call Home Mitigation Request YANG Module

   <CODE BEGINS> file "ietf-dots-signal-call-home@2018-09-28.yang"

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

     import ietf-inet-types {
       prefix inet;
       reference
         "Section 4 of RFC 6991";
     }
     import ietf-dots-signal-channel {
       prefix ietf-signal;
       reference
         "RFC XXXX: 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>";

     description
       "This module contains YANG definition for the signaling
        messages exchanged between a DOTS client and a DOTS server.

        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 2018-09-28 {
      description
        "Initial revision.";
      reference
        "RFC XXXX: Distributed Denial-of-Service Open Threat
                   Signaling (DOTS) Signal Channel Call Home";
    }

    augment "/ietf-signal:dots-signal" {
      when "message-type='mitigation-scope'";
      description "Attacker source 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";
        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.";
        }
      }
    }
  }
```

4. DOTS Data Channel Call Home

4.1. Procedure

Figure 2 shows the main steps that may be observed when a Call Home service is enabled between too peer DOTS agents.

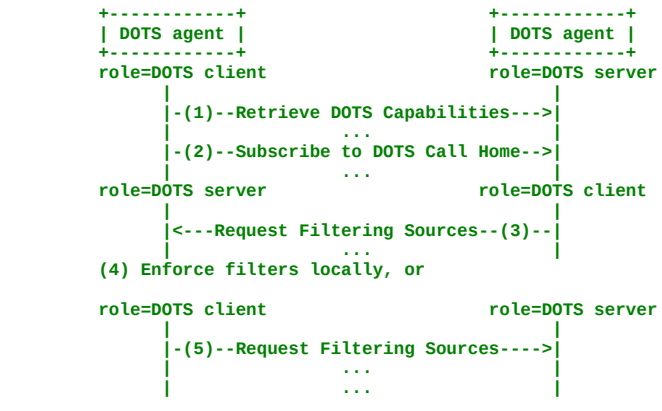

Figure 2: DOTS Call Home: Data Channel Overview

At bootstrapping, the first DOTS agent #1, acting as a DOTS client, contacts its peer DOTS agent #2 (acting as a DOTS server) as per the procedure specified in [I-D.ietf-dots-data-channel]. Then, the DOTS client sends a request to retrieve the capabilities of the peer DOTS agent #2. If that peer agent supports the Call Home service (Section 4.2.1), the DOTS client sends a request to the peer DOTS agent #2 to subscribe to the Call Home service (see Section 4.2.2 for further details).

Once the subscription is validated and put into effect, the DOTS agent #2 may act as a DOTS client at any moment if it detects some suspicious traffic originating from the client domain #1. In order to avoid disrupting the service offered to that domain, DOTS agent #2 sends a request to DOTS agent #1 by means of [I-D.ietf-dots-data-channel] to request some filtering rules to be enforced at the boundaries of the client domain.

Upon receipt of that request, the DOTS agent #1 may enforce the requested filtering rules, relay the request to an administrator, or echo the request back to the DOTS agent #2 as per normal DOTS data channel procedure.

4.2. DOTS Data Channel Extension

4.2.1. DOTS Call Home Capability

As specified in [I-D.ietf-dots-signal-channel], a DOTS client sends a GET request to retrieve the filtering capabilities supported by a DOTS server. Figure 3 shows an example of such request.

```
GET /restconf/data/ietf-dots-data-channel:dots-data\
    /capabilities HTTP/1.1
Host: {host}:{port}
Accept: application/yang-data+json
```

Figure 3: GET to Retrieve the Capabilities of a DOTS Server

A DOTS server which supports the Call Home functionality replies with a response such as the one depicted in Figure 4.

```
Content-Type: application/yang-data+json
{
 "ietf-dots-data-channel:capabilities": {
   "forwarding-actions": ["drop", "accept"],
   "rate-limit": true,
   "transport-protocols": [1, 6, 17, 58],
   "ipv4": {
     "length": true,
     "protocol": true,
     "destination-prefix": true,
     "source-prefix": true,
     "fragment": true
   },
   "ipv6": {
     "length": true,
     "protocol": true,
     "destination-prefix": true,
     "source-prefix": true,
     "fragment": true
   },
   "tcp": {
     "flags-bitmask": true,
     "source-port": true,
     "destination-port": true,
     "port-range": true
   },
   "udp": {
     "length": true,
     "source-port": true,
     "destination-port": true,
     "port-range": true
   },
   "icmp": {
     "type": true,
     "code": true
   }
   "call-home-support": true,
  }
}
```

Figure 4: DOTS Server Capabilities

All the attributes listed in Figure 4 except 'call-home-support', are defined in [I-D.ietf-dots-signal-channel]. The meaning of 'call-home-support' parameter is described below:

call-home-support: This attribute is used by a DOTS server to indicate whether it supports the Call Home functionality, when set to 'true'.

This is an optional attribute.

4.2.2. Registration to The Call Home Service

In order to make use of DOTS Call Home function, a DOTS client MUST register to its DOTS server(s) by creating a DOTS client ('dots-client') resource and setting the 'call-home-enable' parameter to 'true'. To that aim, DOTS clients send a POST request shown in Figure 5.

```
POST /restconf/data/ietf-dots-data-channel:dots-data HTTP/1.1
Host: {host}:{port}
Content-Type: application/yang-data+json
{
  "ietf-dots-data-channel:dots-client": [
    {
      "cuid": "string",
      "call-home-enable": boolean
    }
  ]
}
```

Figure 5: Register to Call Home

The 'call-home-enable' parameter is described below:

call-home-enable: If set to 'true', this means the DOTS client requests subscribing to the DOTS Call Home service.

This is an optional attribute.

A DOTS client can disable its subscription to the Call Home service either by de-registering the 'dots-client' resource or by sending a registration refresh request with 'call-home-enable' set to 'false'.

A DOTS client which subscribed to a Call Home service should be

prepared to receive incoming unsolicited requests from the peer DOTS
agent.

<<<<some text about source port/nat traversal>>>>>>

4.2.3. Tree Structure

This document augments the DOTS data channel YANG module
~~"reddy-dots-home-network", which has the following structure:~~ defined in
[I-D.ietf-dots-data-channel] as follows:

```
module: ~~reddy-dots-home-network~~ ietf-dots-data-call-home
  augment ~~/ietf-signal:dots-signal:~~
~~    +--rw source-prefix*        inet:ip-prefix~~
~~    +--rw source-port-range* [lower-port upper-port]~~ /ietf-data:dots-data/dots-client:
    +--rw ~~lower-port    inet:port-number~~ call-home-enable*       boolean
  augment /ietf-data:dots-data/capabilities:
    +--rw ~~upper-port    inet:port-number~~
```

~~4.2.2. Mitigation Request Model~~ call-home-support* boolean

4.2.4. YANG Module

<CODE BEGINS> file ~~"reddy-dots-home@2018-09-25.yang"~~ "ietf-dots-data-call-home@2018-09-28.yang"

```
module ~~reddy-dots-home-network~~ ietf-dots-data-call-home {
  yang-version 1.1;
  namespace ~~"urn:ietf:params:xml:ns:yang:ietf-dots-signal-channel";~~ "urn:ietf:params:xml:ns:yang:ietf-dots-data-call-home";
  prefix ~~signal;~~ data-call-home;

  import ietf-inet-types {
    prefix inet;
    reference
      "Section 4 of RFC 6991";
  }
  import ~~ietf-dots-signal-channel~~ ietf-dots-data-channel {
    prefix ~~ietf-signal;~~ ietf-data;
    reference
      "RFC XXXX: Distributed Denial-of-Service Open Threat
                 Signaling (DOTS) Data 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:  Mohamed Boucadair
              <mailto:mohamed.boucadair@orange.com>";

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

  description
    "This module contains YANG definition for the signaling
     messages exchanged between a DOTS client and a DOTS server.

     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 ~~2018-09-24~~ 2018-09-28 {
    description
      "Initial revision.";
    reference
      "RFC XXXX: Distributed Denial-of-Service Open Threat
                 Signaling (DOTS) ~~Signal~~ Data Channel ~~Specification";~~ Call Home";
  }

  augment ~~"/ietf-signal:dots-signal"~~ "/ietf-data:dots-data/ietf-data:capabilities" {
    ~~when "message-type='mitigation-scope'";~~
    description ~~"Attacker source details";~~

~~    leaf-list source-prefix~~
      "Augments the DOTS data channel with Call Home capability.";

    leaf call-home-support {
      type ~~inet:ip-prefix;~~ boolean;
      description
        ~~"IPv4 or IPv6 prefix identifying~~
        "DOTS Call Home feature is a capability which is meant
         to allow a home network to receive requests from the ~~attacker.";~~ ISP
         network.";
    }
    ~~list source-port-range~~
  }

  augment "/ietf-data:dots-data/ietf-data:dots-client" {
      ~~key "lower-port upper-port";~~
    when "/ietf-data:dots-data/ietf-data:capabilities/" +
         "data-call-home:call-home-support='true'";
    description
        ~~"Port range. When only lower-port is~~
~~         present, it represents~~
```

```
          "Allows a single port number."; DOTS client to enable/disable Call Home
           functionality.";

        leaf lower-port call-home-enable {
          type inet:port-number;
          mandatory true; boolean;
          description
              "Lower port number of
            "When set to 'true', this means 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 DOTS client registers
             to lower port number.";
        }
        description
            "Upper port number of the port range.";
        } Call Home functionality.";
      }
    }

  }
```

5. IANA Considerations

5.1. 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 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).

5.2. DOTS Signal Channel CBOR Mappings Registry

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

5.2.1. Registry Content

The source-prefix and source-port-range are comprehension-optional parameters.

Parameter Name	YANG Type	CBOR Key	CBOR Major Type & Information	JSON Type
source-prefix	leaf-list inet: ip-prefix	0x8000 (TBD)	4 array 3 text string	Array String
source-port-range	list	0x8001 (TBD)	4 array	Array

Table 4: CBOR Mappings Used in DOTS Signal Channel Messages

5.3. DOTS Signal Channel YANG Module

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

```
        URI: urn:ietf:params:xml:ns:yang:reddy-dots-home-network urn:ietf:params:xml:ns:yang:ietf-dots-signal-call-home
        Registrant Contact: The IESG.
        XML: N/A; the requested URI is an XML namespace.

        URI: urn:ietf:params:xml:ns:yang:ietf-dots-data-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 modules in the "YANG Module Names" registry [RFC7950].

```
      name: ietf-signal ietf-signal-call-home
      namespace: urn:ietf:params:xml:ns:yang:reddy-dots-home-network urn:ietf:params:xml:ns:yang:ietf-dots-signal-call-home
      prefix: signal signal-call-home
      reference: RFC XXXX

      name: ietf-data-call-home
      namespace: urn:ietf:params:xml:ns:yang:ietf-dots-data-call-home
      prefix: data-call-home
      reference: RFC XXXX
```

6. Security Considerations

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

An attacker ~~could~~ **may** launch a ~~denial-of-service (DoS)~~ **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.

7. Acknowledgements

TBC.

8. References

8.1. Normative References

[I-D.ietf-dots-data-channel]
Boucadair, M., K, R., Nishizuka, K., Xia, L., Patil, P., Mortensen, A., and N. Teague, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Data Channel Specification", draft-ietf-dots-data-channel-22 (work in progress), September 2018.

[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-25 (work in progress), September 2018.

[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>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/info/rfc7252>.

[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>.

8.2. 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-15 (work in progress), August 2018.

[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-16 (work in progress), July 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>.

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <https://www.rfc-editor.org/info/rfc7049>.

[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>.

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

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

Email: harsha_joshi@mcafee.com